Dell Data Protection | Enterprise Edition

설치 안내서 v8.13

참고, 주의 및 경고

노트: "참고"는 제품을 보다 효율적으로 사용하는 데 도움이 되는 중요 정보를 제공합니다.

주의: "주의"는 하드웨어 손상이나 데이터 손실의 가능성을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.

경고: "경고"는 재산상의 피해나 심각한 부상 또는 사망을 유발할 수 있는 위험이 있음을 알려줍니다.

Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise 및 Dell Data Guardian 문서 세트에 사용된 등록된 상표 및 상표, 즉 Dell™, Dell 로고, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® 및 KACE™는 Dell Inc. Cylance® 및 CylancePROTECT의 상표이고 Cylance 로고는 미국에서 Cylance, Inc.의 등록된 상표입니다. 상표입니다. McAfee® 및 McAfee 로고는 미국 및 기타 국가에서 McAfee, Inc.의 상표 또는 등록 상표입니다. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® 및 Xeon®은 미국 및 기타 국가에서 Intel Corporation의 등록 상표입니다. Adobe®, Acrobat®, 및 Flash®는 Adobe Systems Incorporated의 등록 상표입니다. Authen Tec® 및 Eikon®은 Authen Tec의 등록 상표입니다. AMD®는 Advanced Micro Devices, Inc.의 등록 상표입니다. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, Visual C++®는 미국 및/또는 기타 국가에서 Microsoft Corporation의 상표 또는 등록 상표입니다. VMware®는 미국 또는 기타 국가에서 VMware, Inc.의 등록 상표 또는 상표입니다. Box®는 Box의 등록 상표입니다. DropboxSM은 Dropbox, Inc.의 서비스 표시입니다. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® 및 Google™ Play는 미국 및 기타 국가에서 Google Inc.의 상표 또는 등록 상표입니다. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® 및 Siri®는 미국 및/또는 기타 국가에서 Apple, Inc.의 서비스 표시, 상표, 또는 등록 상표입니다. GO ID®, RSA®, SecurID®는 Dell EMC의 등록 상표입니다. EnCase™ 및 Guidance Software®는 Guidance Software의 상표 또는 등록 상표입니다. Entrust®는 미국 및 기타 국가에서 Entrust®, Inc.의 등록 상표입니다. InstallShield®는 미국, 중국, 유럽 공동체, 홍콩, 일본, 대만, 및 영국에서 Flexera Software의 등록 상표입니다. Micron® 및 RealSSD®는 미국 및 기타 국가에서 Micron Technology, Inc.의 등록 상표입니다. Mozilla® Firefox®는 미국 및/또는 기타 국가에서 Mozilla Foundation의 등록 상표입니다. iOS®는 미국 및 기타 특정 국가에서 Cisco Systems, Inc.의 상표 또는 등록 상표이며, 라이선스 하에 사용됩니다. Oracle® 및 Java®는 Oracle 및/또는 Oracle 계열사의 등록 상표입니다. 기타 이름은 해당 소유자의 상표일 수 있습니다. SAMSUNG™은 미국 또는 기타 국가에서 SAMSUNG의 상표입니다. Seagate®는 미국 및/또는 기타 국가에서 Seagate Technology LLC의 등록 상표입니다. Travelstar®는 미국 및 기타 국가에서 HGST, Inc.의 등록 상표입니다. UNIX®는 The Open Group의 등록 상표입니다. VALIDITY™는 미국 및 기타 국가에서 Validity Sensors, Inc.의 상표입니다. VeriSign®과 기타 관련 상표는 미국 및 기타 국가에서 VeriSign, Inc.와 그 계열사 또는 자회사의 상표 또는 등록 상표이며, Symantec Corporation에 사용 허가된 상표 또는 등록 상표입니다. KVM on IP®는 Video Products의 등록 상표입니다. Yahoo!®는 Yahoo! Inc.의 등록 상표입니다. 본 제품은 7-Zip 프로그램을 일부 사용합니다. 소스 코드는 7-zip.org에서 찾아볼 수 있습니다. 라이센싱에는 GNU LGPL 라이센스 + unRAR 제한이 적용됩니다(www.7-zip.org/license.txt).

Personal Edition 설치 안내서

2017 - 04

개정 A01

목차

1

Personal Edition 개요

이 안내서는 Security Tools가 Personal Edition과 함께 설치된다는 것을 전제로 합니다.

Personal Edition

Personal Edition의 목적은 컴퓨터를 읽어버리거나 도난당한 이후에도 컴퓨터의 데이터를 보호하기 위한 것입니다.

기밀 데이터의 보안을 보장하기 위해 Personal Edition은 Windows 컴퓨터에 있는 데이터를 암호화합니다. 사용자는 컴퓨터에 로그인한 뒤 언제나 데이터에 액세스할 수 있지만, 허가받지 않은 사용자는 이 보호된 데이터에 액세스할 수 없습니다. 데이터는 항상 드라이브에 암호화된 상태로 유지되지만, 암호화가 투명하기 때문에 사용자가 응용 프로그램 및 데이터를 사용하는 방법을 변경할 필요는 없습니다.

일반적으로 Encryption 클라이언트는 사용자가 작업하는 동안 데이터의 암호를 해독합니다. 경우에 따라서 Encryption 클라이언트가 파일을 암호화하거나 암호 해독할 때 응용 프로그램에서 동시에 파일에 액세스하려고 시도할 수 있습니다. 이 경우 몇 초 후에 Encryption 클라이언트에 암호화/암호 해독을 기다리거나 취소할 수 있는 옵션을 제공하는 대화 상자가 표시됩니다. 기다리는 옵션을 선택하면 Encryption 클라이언트가 완료 직후 파일을 공개합니다(일반적으로 몇 초 내).

Security Tools

Security Tools의 목적은 Advanced Authentication 지원을 위한 종단 간 보안 솔루션을 제공하는 것입니다.

Security Tools는 암호, 지문 판독기 및 스마트 카드("비접촉식"과 "접촉식" 모두)뿐만 아니라 자체 등록, OTP(일회용 암호) 및 원스텝 로그온(SSO[Single Sign-On])을 통해 Windows 인증을 수행할 수 있는 다단계 지원을 제공합니다.

보안 콘솔은 로컬 관리자가 설정한 정책을 기반으로 사용자에게 자격 증명 및 자체 복구 질문을 구성할 수 있도록 안내하는 Security Tools 인터페이스입니다.

관리자 설정 도구는 관리자 권한이 있는 사용자가 사용할 수 있으며, 이를 통해 인증 정책과 복구 옵션을 설정하고, 사용자를 관리하고, 고급 설정과 Windows 로그온을 위해 지원되는 자격 증명에 고유한 설정을 구성할 수 있습니다.

Security Tools 응용 프로그램 사용 방법에 대해서는 Security Tools 관리자 설정 구성 및 *Dell Console 사용 설명서*를 참조하십시오.

Dell ProSupport에 문의

877-459-7304(내선번호 4310039)로 전화하면 연중무휴 하루 24시간 Dell Data Protection 제품에 대한 전화 지원을 받을 수 있습니다.

또한, dell.com/support에서 Dell Data Protection 제품에 대한 온라인 지원도 가능합니다. 온라인 지원에는 드라이버, 매뉴얼, 기술 자문, FAQ 및 최근에 나타나는 문제도 포함됩니다.

올바른 기술 전문가에게 신속히 연결될 수 있도록 전화할 때 서비스 코드를 준비하십시오.

미국 외부의 전화 번호는 Dell ProSupport 국제 전화 번호를 확인하십시오.

2

Personal Edition 요구 사항

이 요구 사항에는 Personal Edition 설치에 필요한 모든 내용이 자세히 설명되어 있습니다.

Encryption 클라이언트

- Personal Edition을 성공적으로 설치하려면 권한 부여가 필요합니다. 권한 부여는 Personal Edition을 구매할 때 제공됩니다. Personal Edition을 어떻게 구매했는지에 따라 수동으로 권한 부여를 설치해야 할 수도 있습니다. 이 경우 권한 부여에 수반되는 간단한 지침을 따르십시오. Personal Edition을 Dell Digital Delivery를 사용하여 설치한 경우에는 Dell Digital Delivery 서비스가 권한 부여 설치를 알아서 처리합니다. (동일한 바이너리가 Enterprise Edition과 Personal Edition에 사용됩니다. 권한 부여는 설치 프로그램이 설치해야 할 버전을 알려줍니다.)
- 암호화된 데이터에 대한 액세스를 보호하기 위해 Windows 암호를 사용하는 것이 좋습니다(없을 경우). 컴퓨터 암호를 만들면 암호를 모르는 다른 사용자가 내 사용자 계정에 로그인할 수 없습니다.
  a Windows 제어판(**시작 > 제어판**)으로 이동합니다
  b **사용자 계정** 아이콘을 클릭합니다.
  c **계정에 대한 암호 생성**을 클릭합니다.
  d 새 암호를 입력하고 다시 한 번 입력합니다.
  e 필요에 따라 암호 힌트를 입력합니다.
  f **암호 생성**을 클릭합니다.
  g 컴퓨터를 다시 시작하십시오.
- 배포 시에는 IT 모범 사례를 따라야 합니다. 예를 들어, 초기 테스트에서 테스트 환경을 통제하고 사용자에 대해 시간별 배포를 수행해야 합니다.
- 설치/업그레이드/설치 제거를 수행하는 사용자 계정은 로컬 또는 도메인 관리자여야 하며, 관리자 권한은 Microsoft SMS 또는 Dell KACE 등의 배포 도구를 사용하여 임시로 할당할 수 있습니다. 관리자 이외의 사용자는 상승된 권한을 가진 경우에도 지원되지 않습니다.
- 설치/설치 제거/업그레이드를 시작하기 전에 중요한 데이터를 모두 백업하십시오.
- 설치/설치 제거/업그레이드가 진행되는 동안에는 외부(USB) 드라이브 삽입 또는 제거를 비롯하여 컴퓨터를 변경하지 마십시오.
- 초기 암호화 시간(및 설치 제거 시 암호 해독 시간)을 줄이려면 Windows 디스크 정리 마법사를 실행하여 임시 파일 및 기타 불필요한 데이터를 모두 제거합니다.
- 암호화 스윕이 처음 실행되는 동안, 사용자가 없는 시간에 컴퓨터가 절전 모드로 전환되지 않도록 절전 모드를 해제하십시오. 절전 상태의 컴퓨터에서는 암호화 및 암호 해독이 발생되지 않습니다.
- 이중 부팅 구성은 다른 운영 체제의 시스템 파일을 암호화하여 작업을 방해할 수 있으므로 Encryption 클라이언트는 이중 부팅 구성을 지원하지 않습니다.
- v8.0 이전 구성 요소는 마스터 설치 프로그램으로 업그레이드할 수 없습니다. 마스터 설치 프로그램에서 하위 설치 프로그램을 추출하고 구성 요소를 개별적으로 업그레이드합니다. 질문이나 우려 사항이 있는 경우 Dell ProSupport에 문의하십시오.
- 이제 Encryption 클라이언트가 Audit 모드를 지원합니다. Audit 모드를 사용하면 관리자는 타사 SCCM 또는 유사 솔루션을 사용하여 Encryption 클라이언트를 배포하는 대신, 암호화 기업 이미지의 일부로서 Encryption 클라이언트를 배포할 수 있습니다. 기업 이미지에 Encryption 클라이언트를 설치하는 방법에 대한 지침은 http://www.dell.com/support/article/us/en/19/SLN304039을 참조하십시오.
- TPM은 GPK 키 봉인에 사용됩니다. 따라서 Encryption 클라이언트를 실행하는 경우, 클라이언트 컴퓨터에 새 운영 체제를 설치하기 전에 BIOS에서 TPM을 삭제하십시오.
- Encryption 클라이언트는 McAfee, Symantec 클라이언트, Kaspersky, MalwareBytes에 맞게 테스트를 거쳤으며 호환 가능합니다. 이러한 바이러스 백신 공급자를 위한 하드 코딩된 제외가 제공되므로 바이러스 백신 스캔과 암호화 간의 불일치를 방지할 수 있습니다. 또한 Encryption 클라이언트는 Microsoft Enhanced Mitigation Experience Toolkit에 맞게 테스트를 거쳤습니다.

  여기에 나열되지 않은 바이러스 백신 공급자를 조직에서 사용하고 있는 경우 KB 문서 SLN298707이나 Dell ProSupport에 연락을 참조하여 도움을 받으십시오.

- Encryption 클라이언트가 설치된 상태에서는 내부 운영 체제 업그레이드가 지원되지 않습니다. Encryption 클라이언트를 설치 제거 및 암호 해독하고, 새 운영 체제로 업그레이드한 후, Encryption 클라이언트를 다시 설치합니다.

  추가적으로 운영 체제 재설치는 지원되지 않습니다. 운영 체제를 재설치하려는 경우 대상 컴퓨터를 백업하고, 컴퓨터를 초기화하고, 운영 체제를 설치한 뒤 다음의 설정된 복구 절차에 따라 암호화된 데이터를 복구합니다.
- www.dell.com/support 에 최신 설명서 및 기술 자문이 있는지 정기적으로 확인하십시오.

Encryption 클라이언트 필수 구성 요소

- 마스터 설치 프로그램 및 하위 설치 프로그램 클라이언트에는 Microsoft .NET Framework 4.5.2 이상이 필요합니다.

  모든 Dell 컴퓨터에는 Microsoft .Net Framework 4.5.2 이상이 기본적으로 설치되어 있습니다. 하지만 Dell 하드웨어에 설치하지 않거나 이전 Dell 하드웨어에서 클라이언트를 업그레이드하는 경우에는, **클라이언트를 설치하기 전에** 어떤 버전의 Microsoft .Net이 설치되어 있는지 확인한 후 버전을 업데이트해야만 설치/업그레이드에 따른 문제를 방지할 수 있습니다. 설치되어 있는 Microsoft .Net의 버전을 확인하려면 설치하고자 하는 컴퓨터에서 다음 지침을 따르십시오: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx Microsoft .Net Framework 4.5.2를 설치하려면 https://www.microsoft.com/en-us/download/details.aspx?id=42643로 이동합니다.
- 마스터 설치 프로그램에서 Microsoft Visual C++ 2012 업데이트 4를 설치합니다(컴퓨터에 이미 설치되어 있지 않은 경우). **하위 설치 프로그램을 사용할 때는** Encryption 클라이언트를 설치하기 전에 이 구성 요소를 설치해야 합니다.

필수 구성 요소

- Visual C++ 2012 업데이트 4 이상의 재배포 가능 패키지(x86 및 x64)
- Microsoft SQL Server Compact 3.5 SP2(x86 및 x64)

Encryption 클라이언트 하드웨어

- 다음 표에 지원되는 컴퓨터 하드웨어가 나와 있습니다.

하드웨어

- 최소 하드웨어 요구 사항은 운영 체제의 최소 사양을 충족시켜야 합니다.

- 다음 표에 지원되는 컴퓨터 하드웨어(선택 사항)가 나와 있습니다.

내장 하드웨어(선택 사항)

- TPM 1.2 또는 2.0

Encryption 클라이언트 운영 체제

- 다음 표에 지원되는 운영 체제가 나와 있습니다.

Windows 운영 체제(32 및 64비트)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7, 응용 프로그램 호환성 템플릿 포함(하드웨어 암호화는 지원되지 않음)
- Windows 8: Enterprise, Pro
- Windows 8.1 업데이트 0-1: Enterprise Edition, Pro Edition
- Windows Embedded 8.1 Industry Enterprise (하드웨어 암호화는 지원되지 않음)
- Windows 10: Education, Enterprise, Pro
- VMware Workstation 5.5 이상

Windows 운영 체제(32 및 64비트)

노트: UEFI 모드는 Windows 7, Windows Embedded Standard 7 또는 Windows Embedded 8.1 Industry Enterprise에서 지원되지 않습니다.

EMS(External Media Shield)용 운영 체제

- 다음 표에는 EMS로 보호되는 미디어에 대한 액세스가 지원되는 운영 체제가 자세히 나와 있습니다.

노트: EMS를 호스팅하려면 외장형 미디어에 약 55MB의 사용 가능한 공간과 암호화할 파일 중 최대 크기의 파일에 해당하는 여유 공간이 있어야 합니다.

노트:

Windows XP는 EMS Explorer를 사용할 때만 지원됩니다.

EMS로 보호받는 미디어(32 및 64비트)에 대한 액세스가 지원되는 Windows 운영 체제

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate, Home Premium
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 업데이트 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

EMS로 보호되는 미디어에 대한 액세스가 지원되는 Mac 운영 체제(64비트 커널)

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.0

Encryption 클라이언트 언어 지원

- Encryption 클라이언트는 MUI(다국어 사용자 인터페이스)와 호환되며 다음 언어를 지원합니다.

언어 지원

- EN - 영어
- ES - 스페인어
- FR - 프랑스어
- IT - 이탈리아어
- DE - 독일어
- JA - 일본어
- KO - 한국어
- PT-BR - 포르투갈어, 브라질
- PT-PT - 포르투갈어, 포르투갈(이베리아)

Advanced Authentication 클라이언트

- Advanced Authentication을 통해 Security Tools를 사용하여 관리 및 등록하는 Advanced Authentication 자격 증명을 사용하여 이 컴퓨터에 사용자가 안전하게 액세스할 수 있습니다. Security Tools는 Windows 암호, 지문, 스마트 카드를 포함한 Windows 로그인에 대한 인증 자격 증명의 기본 관리자가 됩니다. Microsoft 운영 체제를 사용하여 등록한 사진 암호, PIN, 지문 자격 증명은 Windows 로그인 시 인식되지 않습니다.

  계속해서 Microsoft 운영 체제를 사용하여 사용자의 자격 증명을 관리하려면 Security Tools를 설치하거나 설치 제거하지 마십시오.

- Security Tools OTP(일회용 암호) 기능을 사용하려면 TPM을 설치하고, 활성화해야 하며, 소유권을 가지고 있어야 합니다. OTP는 TPM 2.0에서 지원되지 않습니다. TPM의 소유권을 제거한 후 설정하려면 https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2를 참조하십시오.

Advanced Authentication Client 하드웨어

- 다음 표에는 지원되는 인증 하드웨어가 자세히 설명되어 있습니다.

지문 및 스마트 카드 판독기

- 보안 모드의 Validity VFS495
- Dell ControlVault 스와이프 리더
- UPEK TCS1 FIPS 201 보안 리더 1.6.3.379
- Authentec Eikon 및 Eikon To Go USB 리더

비접촉식 카드

- 지정된 Dell 랩톱에 탑재된 비접촉식 카드 리더기를 이용한 비접촉식 카드

스마트 카드

- ActivIdentity 클라이언트를 사용하는 PKCS #11 스마트 카드

  노트: ActivIdentity 클라이언트는 사전 로드되어 있지 않으며 별도로 설치해야 합니다.
- CSP 카드
- CAC(Common Access Cards)
- 클래스 B/SIPR Net 카드

- Dell ControlVault용 드라이버 및 펌웨어, 지문 판독기 및 스마트 카드는(아래 참조) 마스터 설치 프로그램 또는 하위 설치 프로그램 실행 파일에 포함되어 있지 않습니다. 드라이버 및 펌웨어는 최신 상태로 유지해야 하며 http://www.dell.com/support에서 해당 컴퓨터 모델을 선택하여 다운로드할 수 있습니다. 인증 하드웨어에 따라 적절한 드라이버 및 펌웨어를 다운로드하십시오.

  - Dell ControlVault
  - NEXT 생채 인식 지문 드라이버
  - 유효 지문 판독기 495 드라이버
  - O2Micro 스마트 카드 드라이버

  Dell 이외의 하드웨어에 설치하는 경우 해당 벤더의 웹 사이트에서 업데이트된 드라이버 및 펌웨어를 다운로드하십시오. Dell ControlVault 드라이버 설치 지침은 Dell ControlVault Drivers에 있습니다.
- 다음은 SIPR Net 카드가 지원되는 Dell 컴퓨터 모델을 보여주는 표입니다.

Dell 컴퓨터 모델 - 클래스 B/SIPR Net 카드 지원

- Latitude E6440
- Latitude E6540
- Precision M2800
- Precision M4800
- Precision M6800
- Latitude 14 Rugged Extreme
- Latitude 12 Rugged Extreme
- Latitude 14 Rugged

Advanced Authentication Client 운영 체제

Windows 운영 체제

- 다음 표에 지원되는 운영 체제가 나와 있습니다.

Windows 운영 체제(32 및 64비트)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro
- Windows 8.1 업데이트 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

ⓘ | **노트: UEFI 모드는 Windows 7에서 지원되지 않습니다.**

모바일 장치 운영 체제

- 다음 모바일 운영 체제들은 Security Tools 일회용 암호 기능을 지원합니다.

Android 운영 체제

- 4.0 - 4.0.4 Ice Cream Sandwich
- 4.1 - 4.3.1 Jelly Bean
- 4.4 - 4.4.4 KitKat
- 5.0 - 5.1.1 Lollipop

iOS 운영 체제

- iOS 7.x
- iOS 8.x

Windows Phone 운영 체제

- Windows Phone 8.1
- Windows 10 Mobile

Advanced Authentication Client 언어 지원

- Advanced Authentication 클라이언트는 MUI(다국어 사용자 인터페이스)와 호환되며 다음 언어를 지원합니다. UEFI 모드와 부팅 전 인증은 러시아어, 중국어(번체) 또는 중국어(간체)로 지원되지 않습니다.

언어 지원

- EN - 영어
- FR - 프랑스어
- IT - 이탈리아어
- DE - 독일어
- ES - 스페인어
- JA - 일본어
- KO - 한국어
- ZH-CN - 중국어(간체)
- ZH-TW - 중국어(번체)/대만
- PT-BR - 포르투갈어, 브라질
- PT-PT - 포르투갈어, 포르투갈(이베리아)
- RU - 러시아어

소프트웨어 가져오기로 진행합니다.

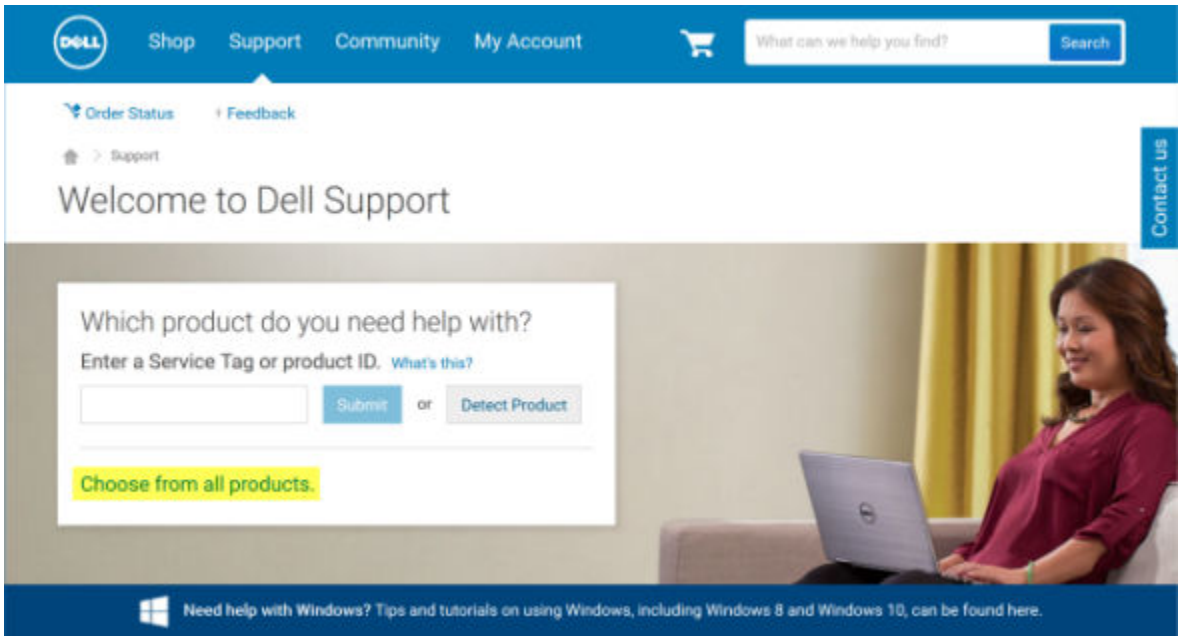
3

소프트웨어 다운로드

이 섹션에서는 dell.com/support에서 소프트웨어를 다운로드하는 방법에 대해 자세히 설명합니다. 이미 소프트웨어가 있는 경우 이 섹션을 건너뛰십시오.

시작하려면 dell.com/support로 이동합니다.

1 Dell 지원 웹 페이지에서 **모든 제품에서 선택**을 선택합니다.



2 제품의 목록에서 소프트웨어 및 보안을 선택합니다.

3 소프트웨어 및 보안 섹션에서 **종단점 보안 솔루션**을 선택합니다.
한 번 선택하고 나면 선택 내용이 웹사이트에 기억됩니다.

4 Dell Data Protection 제품을 선택합니다.
예:

Dell Encryption

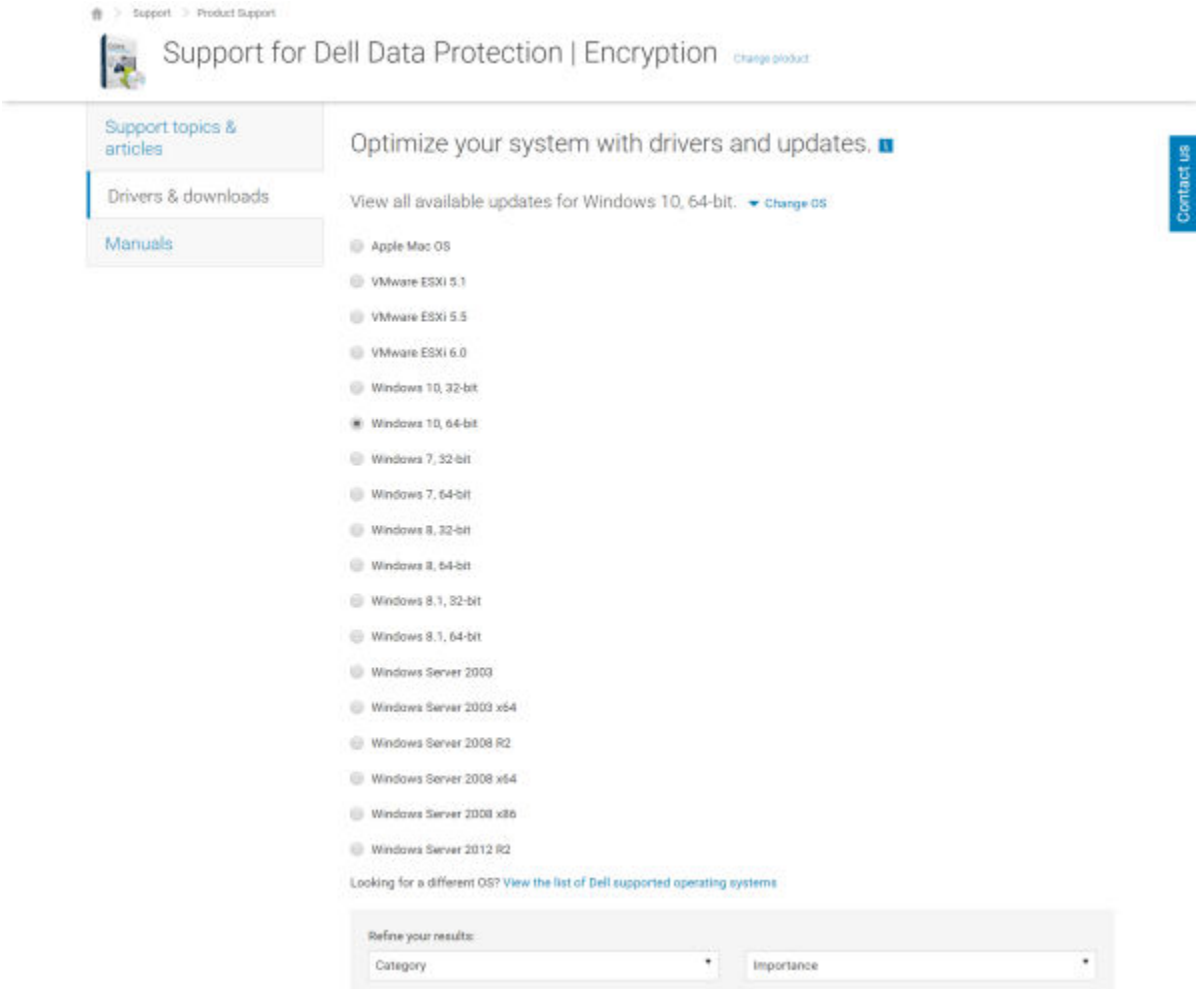
Dell Endpoint Security Suite

Dell Endpoint Security Suite Enterprise

5 **드라이버 및 다운로드**를 선택합니다.

6 원하는 클라이언트 운영 체제 유형을 선택합니다.

7 일치하는 내용에서 **Dell 데이터 보호(4개 파일)**을 선택합니다. 다음은 예일 뿐이므로 실제 모습은 조금 다를 수 있습니다. 예를 들어, 선택 가능한 파일이 4개가 아닐 수 있습니다.



8 **파일 다운로드**를 선택하거나 **내 다운로드 목록 #XX에 추가**를 선택합니다.
개인 Edition 설치를 계속 진행하십시오.

4

Personal Edition 설치

Personal Edition은 마스터 설치 프로그램을 사용하여 설치하거나(권장) 마스터 설치 프로그램에서 하위 설치 프로그램을 추출하여 설치할 수 있습니다. 두 방법 모두 각 조직에 지원되는 푸시 기술을 사용하여 사용자 인터페이스나 명령줄, 또는 스크립트로 설치할 수 있습니다.

응용 프로그램에 대한 도움을 받으려면 사용자는 다음과 같은 도움말 파일을 참조해야 합니다.

- Encryption 클라이언트의 기능 사용 방법에 대해서는 *Dell 암호화 도움말*을 참조하십시오. **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**에 있는 도움말에 액세스하십시오.
- External Media Shield의 기능 사용 방법에 대해서는 *EMS 도움말*을 참조하십시오. **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**에 있는 도움말에 액세스하십시오.
- Advanced Authentication의 기능 사용 방법에 대해서는 *Security Tools 도움말* 을 참조하십시오. **<Install dir>:\Program Files\Dell\Dell Data Protection\Security Tools \Help**에 있는 도움말에 액세스하십시오.

설치 방법 선택

클라이언트를 설치하는 방법은 두 가지입니다. 다음 중 **하나**를 선택하십시오.

- 마스터 설치 프로그램을 사용하여 Personal Edition 설치 - 권장
- 하위 설치 프로그램을 사용하여 Personal Edition 설치

마스터 설치 프로그램을 사용하여 Personal Edition 설치 - 권장

설치 프로그램이 Personal Edition을 설치하려면 컴퓨터에서 적절한 권한 부여를 찾아야 합니다. 적절한 권한 부여가 검색되지 않으면 Personal Edition을 설치할 수 없습니다.

Dell Data Protection 설치 프로그램은 일반적으로 여러 클라이언트를 설치하기 때문에 마스터 설치 프로그램이라고 합니다. Personal Edition의 경우에는 Encryption 클라이언트와 Advanced Authentication을 설치합니다.

마스터 설치 프로그램 사용자 인터페이스를 사용하여 설치할 경우 Personal Edition을 한 번에 한 대의 컴퓨터에만 설치할 수 있습니다.

마스터 설치 프로그램 로그 파일은 **C:\ProgramData\Dell\Dell Data Protection\Installer**에 있습니다.

다음 중 하나의 방법을 선택하십시오.

사용자 인터페이스를 사용하여 설치

명령줄을 사용하여 설치

사용자 인터페이스를 사용하여 설치

필요한 경우 대상 컴퓨터에 권한 부여를 설치하십시오.

DDPSetup.exe를 로컬 컴퓨터로 복사합니다.

DDPSetup.exe를 더블 클릭하여 설치 프로그램을 시작합니다.

필수 구성 요소 설치 상태를 알리는 대화 상자가 표시됩니다. 이 작업은 몇 분 정도 걸립니다.

시작 화면에서 **다음**을 클릭합니다.

라이센스 계약을 읽고 약관에 동의한 후 **다음**을 클릭합니다.

다음을 클릭하여 기본 위치인 **C:\Program Files\Dell\Dell Data Protection**에 Personal Edition을 설치합니다.

Security Tools는 기본적으로 설치되며 선택을 취소할 수 없습니다. 이러한 항목은 설치 프로그램에 Security Framework로 나열됩니다.

Advanced Authentication은 기본적으로 설치되며 선택을 취소할 수 없습니다.

다음을 클릭합니다.

설치를 클릭하여 설치를 시작합니다.

상태 창이 표시됩니다. 이 작업은 몇 분 정도 걸립니다.

Yes, I want to restart my computer now(예, 컴퓨터를 지금 다시 시작합니다)를 선택하고 **마침**을 클릭합니다.

컴퓨터가 다시 시작되면 Windows를 인증합니다.

Personal Edition + Security Tools 설치가 완료됩니다.

Personal Edition 설정 마법사와 구성은 개별적으로 적용됩니다.

Personal Edition 설정 마법사와 구성이 완료되면 Security Tools 관리자 콘솔을 시작합니다.

이 섹션의 다음 부분은 설치 작업을 더 자세히 설명하며, 여기에 대해서는 건너뛰어도 좋습니다. Security Tools 및 Personal Edition 설정 마법사로 진행합니다.

명령줄을 사용하여 설치

필요한 경우 대상 컴퓨터에 권한 부여를 설치하십시오.

스위치:

명령줄 설치를 하려면 가장 먼저 스위치를 지정해야 합니다. 다음 표에 설치 시 사용할 수 있는 스위치 정보가 나와 있습니다.

스위치	의미
-y -gm2	자체 추출기로 데이터 전달
/S	자동 모드
/z	InstallScript 시스템 변수 CMDLINE으로 데이터 전달

매개변수:

다음 표에 설치 시 사용할 수 있는 매개 변수 정보가 나와 있습니다.

매개 변수
InstallPath=설치 위치를 대체하기 위한 경로
FEATURE=PE

명령줄 설치 예

이 예에서는 재부팅을 수행하지 않지만 최종 재부팅은 필요합니다. 컴퓨터를 재부팅해야만 암호화가 시작됩니다.

공백과 같은 특수 문자를 하나 이상 포함하는 값은 이스케이프된 따옴표 안에 포함해야 합니다.

명령줄은 대소문자를 구분합니다.

다음 예에서는 Personal Edition 및 Security Tools를 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
DDPSetup.exe -y -gm2 /S /z"\"FEATURE=PE\""
```

다음 예에서는 Personal Edition 및 Security Tools를 설치합니다(자동 설치, 재부팅하지 않음, 대체 위치인 C:\Program Files\Dell\My_New_Folder에 설치됨).

```
DDPSetup.exe -y -gm2 /S /z"\"FEATURE=PE, InstallPath=C:\Program Files\Dell\My_New_Folder\""
```

컴퓨터가 다시 시작되면 Windows로 인증합니다.

Personal Edition + Security Tools 설치가 완료됩니다.

Personal Edition 설정 마법사와 구성은 개별적으로 적용됩니다.

Personal Edition 설정 마법사와 구성이 완료되면 Security Tools 관리자 콘솔을 시작합니다.

이 섹션의 다음 부분은 설치 작업을 더 자세히 설명하며, 여기에 대해서는 건너뛰어도 좋습니다. Security Tools 및 Personal Edition 설정 마법사로 진행합니다.

하위 설치 프로그램을 사용하여 Personal Edition 설치

하위 설치 프로그램을 사용하여 Personal Edition을 설치하려면 먼저 마스터 설치 프로그램에서 하위 실행 파일을 추출해야 합니다. 마스터 설치 프로그램에서 하위 설치 프로그램 추출을 참조합니다. 완료되면 이 섹션으로 돌아옵니다.

명령줄 설치

명령줄 스위치 및 매개 변수는 대/소문자를 구분합니다.

명령줄에서 공백과 같은 특수 문자를 하나 이상 포함하는 값은 이스케이프된 따옴표로 묶어야 합니다.

이러한 설치 프로그램을 사용하여 스크립팅된 설치, 배치 파일 또는 조직에 제공되는 다른 푸시 기술을 통해 클라이언트를 설치합니다.

명령줄 예에서는 재부팅을 수행하지 않았습니다. 하지만 실제 상황에서는 재부팅이 필요합니다. 컴퓨터를 재부팅해야만 암호화가 시작됩니다.

로그 파일: Windows는 로그인된 사용자에 대해 고유한 하위 설치 프로그램 설치 로그 파일을 C:\Users\<UserName>\AppData\Local\Temp의 %temp%에 생성합니다.

설치 프로그램을 실행할 때 별도의 로그 파일을 추가하려는 경우, 하위 설치 프로그램이 첨부되지 않으므로 해당 로그 파일의 이름은 고유해야 합니다. 표준 .msi 명령을 통해 **/l*v C:\<any directory>\<any log file name>.log**를 사용하여 로그 파일을 생성할 수 있습니다.

별도로 표시된 경우를 제외하고, 모든 하위 설치 프로그램은 명령줄 설치에 동일한 기본 .msi 스위치와 표시 옵션을 사용합니다. 스위치를 먼저 지정해야 합니다. /v 스위치가 필요하며 인수를 사용합니다. 다른 매개 변수는 인수 안에 포함되어 /v 스위치로 전달됩니다.

표시 옵션은 예상 동작을 수행하도록 /v 스위치에 전달된 인수 끝에 지정할 수 있습니다. 동일한 명령줄에 /q와 /qn을 동시에 사용하지 마십시오. /qb 이후에 ! 및 - 만 사용합니다.

스위치	의미
/v	변수를 *.exe 내의 .msi로 전달
/s	자동 모드
/i	설치 모드

옵션	의미
/q	진행률 대화 상자가 없습니다. 프로세스 완료 후 자동으로 다시 시작합니다.
/qb	**취소** 단추가 있는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/qb-	**취소** 단추가 있는 진행률 대화 상자로, 프로세스 완료 후 자동으로 다시 시작합니다.
/qb!	**취소** 단추가 없는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/qb!-	**취소** 단추가 없는 진행률 대화 상자로, 프로세스 완료 후 자동으로 다시 시작합니다.

옵션	의미
/qn	사용자 인터페이스 없음

드라이버 설치

Dell ControlVault용 드라이버 및 펌웨어, 지문 판독기 및 스마트 카드는 마스터 설치 프로그램 또는 하위 설치 프로그램 실행 파일에 포함되어 있지 **않습니다**. 드라이버 및 펌웨어는 최신 상태로 유지해야 하며 http://www.dell.com/support에서 해당 컴퓨터 모델을 선택하여 다운로드할 수 있습니다. 인증 하드웨어에 따라 적절한 드라이버 및 펌웨어를 다운로드하십시오.

Dell ControlVault
NEXT 생채 인식 지문 드라이버
유효 지문 판독기 495 드라이버
O2Micro 스마트 카드 드라이버

Dell 이외의 하드웨어에 설치하는 경우 해당 벤더의 웹 사이트에서 업데이트된 드라이버 및 펌웨어를 다운로드하십시오.

다음 작업:

Advanced Authentication 클라이언트 설치

사용자가 Windows 인증서를 사용하여 PBA에 로그인합니다.

C:\extracted\Security Tools 및 **C:\extracted\Security Tools\Authentication에서 파일을 찾습니다.**

명령줄 설치 예

\Security Tools

다음 예에서는 Security Framework를 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
EMAgent_XXbit_setup.exe /s /v"/norestart /qn"
```

:
이 클라이언트는 v8.x에서 Advanced Authentication에 필요합니다.

다음 작업:

\Security Tools\Authentication

다음 예에서는 Security Tools를 설치합니다(자동 설치, 재부팅하지 않음, 기본 위치인 C:\Program Files\Dell\Dell Data Protection에 설치됨).

```
setup.exe /s /v"/norestart /qn"
```

다음 작업:

Encryption 클라이언트 설치

조직에서 EnTrust 또는 Verisign 등과 같은 루트 인증 기관이 서명한 인증서를 사용하는 경우 Encryption 클라이언트 요구 사항을 검토하십시오. 인증서 유효성 검사를 사용하려면 클라이언트 컴퓨터에서 레지스트리 설정을 변경해야 합니다.

C:\extracted\Encryption에서 파일을 찾습니다.

명령줄 설치 예

다음 예에서는 Personal Edition, Encrypt for Sharing을 설치합니다(오버레이 아이콘 숨김, 대화 상자 없음, 진행률 표시줄 없음, 다시 시작하지 않음).

```
DDPE_XXbit_setup.exe /s /v"HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

컴퓨터가 다시 시작되면 Windows로 인증합니다.

Personal Edition + Security Tools 설치가 완료됩니다. Personal Edition 설정 마법사와 구성은 개별적으로 적용됩니다.

Security Tools 및 Personal Edition 설정 마법사로 진행합니다.

Security Tools 및 Personal Edition 설정 마법사

Windows 사용자 이름 및 암호로 로그온합니다. Windows로 문제 없이 통과됩니다. 인터페이스는 평소 보던 모습과 다를 수 있습니다.

1 UAC에서 응용 프로그램을 실행하라는 메시지가 나타날 수 있습니다. 이 경우, Yes(예)를 클릭합니다.

2 초기 설치 재부팅 후, Security Tools 활성화 마법사가 표시됩니다. **Next(다음)**를 클릭합니다.

3 새 EAP(암호화 관리자 암호)를 입력한 후 다시 한 번 입력합니다. **Next(다음)**를 클릭합니다.

4 복구 정보를 저장하려면 네트워크 드라이브 또는 이동식 미디어의 백업 위치를 입력하고 **Next(다음)**를 클릭합니다.

5 **Apply(적용)**를 클릭하여 ST 활성화를 시작합니다.

6 Security Tools 활성화 마법사가 완료되면, 시스템 트레이의 DDP 아이콘에서 Personal Edition 설정 마법사를 시작합니다(자동 시작될 수도 있음).

이 설정 마법사를 통해 암호화를 사용하여 컴퓨터의 정보를 보호할 수 있습니다. 이 마법사가 완료되지 않으면, 암호화가 시작될 수 없습니다.

시작 화면을 읽고 **Next(다음)**를 클릭합니다.

7 정책 템플릿을 선택합니다. 정책 템플릿이 암호화를 위한 기본 정책 설정으로 적용됩니다.

손쉽게 다른 정책 템플릿을 적용하거나 초기 구성이 완료된 후 로컬 관리 콘솔에서 선택한 템플릿을 사용자 지정할 수 있습니다.

Next(다음)를 클릭합니다.

8 Windows 암호 경고를 읽고 확인합니다. 지금 Windows 암호를 생성하려면 요구 사항을 참조하십시오.

9 9~32자의 EAP(Encryption Administrator Password)를 생성하고 확인합니다. 암호에 영문자, 숫자 및 특수 문자를 포함해야 합니다. 이 암호는 Security Tools에 설정한 EAP와 동일할 수 있으나 이와 관련된 것은 아닙니다. **이 암호를 기록해서 안전한 장소에 보관하십시오**. **Next(다음)**를 클릭합니다.

10 **Browse(찾아보기)**를 클릭하여 암호화 키(LSARecovery_[hostname].exe라는 응용 프로그램에 래핑되어 있음)를 백업하기 위한 네트워크 드라이브 또는 이동식 저장소를 선택합니다.

특정 컴퓨터 장애가 발생할 경우 이러한 키를 사용하여 데이터를 복구합니다.

또한 향후 정책 변경 시 암호화 키를 다시 백업해야 할 수 있습니다. 네트워크 드라이브 또는 이동식 저장소를 사용할 수 있을 경우 암호화 키 백업이 백그라운드에서 수행됩니다. 하지만 위치를 사용할 수 없을 경우에는(예: 원본 이동식 저장 장치가 컴퓨터에 삽입되어 있지 않은 경우) 암호화 키를 수동으로 백업할 때까지 정책 변경이 적용되지 않습니다.

> **노트: 암호화 키를 수동으로 백업하는 방법을 알아보려면 로컬 관리 콘솔 오른쪽 상단 모서리에 있는 "? > 도움말"을 클릭하거나 시작 > 모든 프로그램 > Dell > Dell Data Protection > Encryption > Encryption 도움말을 클릭하십시오.**

Next(다음)를 클릭합니다.

11 암호화 설정 확인 화면에 암호화 설정 목록이 표시됩니다. 항목을 검토한 후 설정에 만족하면 **Confirm(확인)**을 클릭합니다.

컴퓨터 구성이 시작됩니다. 상태 표시줄에 구성 진행률이 표시됩니다.

12 **Finish(마침)**를 클릭하여 구성을 완료합니다.

13 암호화를 위해 컴퓨터를 구성하고 나면 재부팅이 필요합니다. **Reboot Now**(지금 재부팅)를 클릭하거나 재부팅을 각각 5x20분 연기할 수 있습니다.

14 컴퓨터를 재부팅한 뒤 시작 메뉴에서 로컬 관리 콘솔을 열어서 암호화 상태를 봅니다.

백그라운드에서 암호화가 실행됩니다. 로컬 관리자 콘솔은 열거나 닫을 수 있습니다. 두 경우 모두 파일 암호화가 계속 진행됩니다. 암호화 중에도 계속해서 컴퓨터를 사용할 수 있습니다.

15 스캔이 완료되면 컴퓨터가 다시 재부팅됩니다.

모든 암호화 스윕 및 재부팅이 완료되면 로컬 관리자 콘솔을 시작하여 준수 상태를 확인할 수 있습니다. 드라이브는 "In Compliance(준수)" 레이블이 지정됩니다.

Security Tools 관리자 설정 구성으로 진행합니다.

6

Security Tools 관리자 설정 구성

관리자와 사용자는 Security Tools를 활성화한 후 추가 구성 없이 Security Tools 기본 설정을 통해 Security Tools를 바로 사용할 수 있습니다. 사용자가 Windows 암호를 입력하여 컴퓨터에 로그온하면 자동으로 Security Tools 사용자로 추가되지만 다단계 Windows 인증은 기본적으로 비활성화되어 있습니다.

Security Tools 기능을 구성하려면 컴퓨터의 관리자 권한이 필요합니다.

관리자 암호 및 백업 위치 변경

Security Tools를 활성화한 후 필요한 경우 관리자 암호와 백업 위치를 변경할 수 있습니다.

1 관리자가 데스크톱 바로 가기에서 Security Tools를 실행합니다.
2 **관리자 설정** 타일을 클릭합니다.
3 인증 대화 상자에서 활성화 도중 설정한 관리자 암호를 입력한 다음 **확인**을 클릭합니다.
4 **관리자 설정** 탭을 클릭합니다.
5 관리자 암호 변경 페이지에서 암호를 변경하고 싶다면 새 암호를 입력합니다. 새 암호는 8~32자로 문자, 숫자 및 특수 문자가 각각 하나 이상 포함되어야 합니다.
6 확인을 위해 암호를 한 번 더 입력한 다음 **적용**을 클릭합니다.
7 복구 키의 저장 위치를 변경하려면 왼쪽 창에서 **백업 위치 변경**을 선택합니다.
8 새로운 백업 위치를 선택하고 **적용**을 클릭합니다.
   백업 파일을 네트워크 드라이브 또는 이동식 미디어에 저장해야 합니다. 백업 파일에는 이 컴퓨터의 데이터를 복구하는 데 필요한 키가 포함되어 있습니다. 따라서 Dell ProSupport가 데이터 복구를 지원하려면 이 파일에 대한 액세스 권한이 필요합니다.

   복구 데이터는 지정 위치로 자동 백업됩니다. 위치를 사용할 수 없는 경우(예: 백업 USB 드라이브를 삽입하지 않은 경우) Security Tools가 데이터를 백업할 위치를 묻는 메시지를 표시합니다. 암호화를 시작하려면 복구 데이터에 액세스해야 합니다.

인증 옵션 구성

관리자 설정 인증 탭의 컨트롤을 사용하여 사용자 로그인 옵션을 설정하고 각각에 대한 설정값을 사용자 지정할 수 있습니다.

노트: OTP(일회용 암호) 옵션은 TPM의 설치, 활성화, 소유권이 갖춰져 있지 않으면 복구 옵션에 표시되지 않습니다.

로그인 옵션 구성

로그인 옵션 페이지에서는 로그온 정책을 구성할 수 있습니다. 기본적으로 지원되는 모든 자격 증명은 사용 가능한 옵션에 표시됩니다.

로그인 옵션 구성 방법:

왼쪽 창의 인증에서 **로그인 옵션**을 선택합니다.
설정하려는 역할을 선택하려면 **로그인 옵션 적용 대상** 목록에서 **사용자** 또는 **관리자**를 선택합니다. 이 페이지의 변경 사항은 모두 선택한 역할에만 적용됩니다.
인증 시 사용 가능한 옵션을 설정합니다.

기본적으로 각각의 인증 방법은 다른 인증 방법과 함께 사용하지 않고 개별적으로 사용하도록 구성되어 있습니다. 다음과 같은 방법으로 기본값을 변경할 수 있습니다.

인증 옵션의 조합을 설정하려면 사용 가능한 옵션 아래에서 ⁄을 클릭하여 첫 번째 인증 방법을 선택합니다. 사용 가능한 옵션 대화 상자에서 두 번째 인증 방법을 선택하고 **확인**을 클릭합니다.

예를 들어, 로그온 자격 증명으로 지문과 암호를 모두 요청할 수 있습니다. 대화 상자에서, 지문 인증을 통해 사용해야 하는 두 번째 인증 방법을 선택합니다.

각 인증 방법을 개별적으로 사용할 수 있도록 하려면 사용 가능한 옵션 대화 상자에서 두 번째 인증 방법을 **적용 안 함**으로 설정된 채로 두고 **확인**을 클릭합니다.

로그인 옵션을 제거하려면 사용 가능한 옵션의 로그인 옵션 페이지에서 **X**를 클릭하고 인증 방식을 제거할 수 있습니다.

새로운 조합의 인증 방식을 추가하려면 **옵션 추가**를 클릭합니다.

사용자가 잠금 해제되어 컴퓨터 액세스를 복구하려고 할 때는 다음과 같이 복구 옵션을 설정합니다.

사용자가 컴퓨터에 대한 액세스 권한을 다시 얻기 위해 사용할 질문 및 답변을 정의하려면 **복구 질문**을 선택합니다.

복구 질문을 사용하지 않으려면 이 옵션을 선택 취소합니다.

사용자가 모바일 장치를 사용해 액세스 권한을 복구하도록 하려면 **OTP(일회용 암호)**를 선택합니다. OTP(일회용 암호)를 복구 방법으로 선택할 경우 Windows 로그온 화면의 로그인 옵션으로 사용할 수는 없습니다.

OTP 기능을 로그온 옵션으로 사용하려면 복구 옵션에서 이 옵션을 선택 취소하십시오. OTP 기능을 복구 옵션에서 선택 취소하면 OTP에 등록된 사용자가 한 명만 있더라도 OTP 옵션이 Windows 로그온 페이지에 표시됩니다.

: 관리자는 OTP 사용 방법을 인증 또는 복구 목적으로 제어할 수 있습니다. OTP 기능은 인증이나 복구 목적으로 사용할 수도 있지만, 이 두 가지를 동시에 지원하지는 못합니다. 로그인 옵션 필드인 로그인 옵션 적용 대상에서 선택한 항목에 따라 컴퓨터의 모든 사용자 또는 모든 관리자에게 구성이 적용됩니다.

복구 옵션 아래에 일회용 암호 옵션이 나열되지 않으면 컴퓨터의 구성에서 이 옵션을 지원하지 않는 것입니다. 자세한 내용은 요구 사항을 참조하십시오.

사용자가 로그온 자격 증명을 잊거나 잃어버린 경우 헬프 데스크로 연락하도록 하려면 복구 옵션 아래에서 복구 질문과 일회용 암호 확인란을 모두 선택 취소합니다.

사용자가 인증 자격 증명을 등록할 수 있는 기간을 설정하려면 **유예 기간**을 선택합니다.

유예 기간 기능을 통해, 구성된 로그인 옵션의 적용 시작일을 선택할 수 있습니다. 로그인 옵션 적용 날짜 이전에 이를 구성하고, 사용자의 등록 기간을 설정할 수 있습니다. 기본적으로 이 정책은 즉시 적용됩니다.

로그인 옵션 적용 날짜를 *즉시*에서 다른 날짜로 변경하려면 유예 기간 대화 상자에서 드롭다운 메뉴를 클릭하고 **지정된 날짜**를 선택합니다. 날짜 필드의 오른쪽에 있는 아래쪽 화살표를 클릭하여 달력을 표시하고 날짜를 선택합니다. 정책은 선택한 날짜의 약 오전 12시 1분부터 시작됩니다.

사용자는 다음에 Windows에 로그온할 때 필요한 자격 증명을 등록하라는 알림을 수신할 수도 있고(기본값), 정기적인 미리 알림을 설정할 수도 있습니다. *사용자에게 알림* 드롭다운 목록에서 미리 알림 간격을 선택합니다.

:

사용자에게 표시되는 미리 알림은 미리 알림이 트리거되었을 때 사용자가 Windows 로그온 화면에 있는지 또는 Windows 세션 안에 있는지에 따라 약간 다릅니다. 부팅 전 인증 로그온 화면에는 미리 알림이 나타나지 않습니다.

유예 기간 중 기능

지정된 유예 기간 동안 사용자가 변경된 로그인 옵션을 충족하는 데 필요한 최소 자격 증명을 등록하지 않았으면 로그인할 때마다 추가 자격 증명 알림이 표시됩니다. 메시지에는 *'추가 자격 증명을 등록할 수 있습니다.'*라는 내용이 표시됩니다.

추가 자격 증명을 사용할 수 있지만 필수 사항은 아닌 경우 정책이 변경된 후 메시지가 한 번만 표시됩니다.

알림을 클릭하면 컨텍스트에 따라 다음과 같은 결과가 나타납니다.

등록된 자격 증명이 없는 경우 관리자는 컴퓨터 관련 설정을 구성하고 사용자는 가장 일반적인 자격 증명을 등록할 수 있는 설정 마법사가 표시됩니다.

처음으로 자격 증명을 등록한 후 알림을 클릭하면 DDP 보안 콘솔 내에 설정 마법사가 표시됩니다.

유예 기간 만료 후 기능

유예 기간이 만료되면 로그인 옵션에서 요구하는 자격 증명을 등록해야만 로그온할 수 있습니다. 사용자가 로그인 옵션을 충족하지 않는 자격 증명 또는 자격 증명의 조합으로 로그온하도록 시도하면 Windows 로그온 화면 위에 설정 마법사가 표시됩니다.

사용자가 필요한 자격 증명을 성공적으로 등록하면 Windows에 로그인됩니다.

사용자가 필요한 자격 증명을 성공적으로 등록하지 않거나 마법사를 취소하면 Windows 로그온 화면으로 돌아갑니다.

선택한 역할에 대한 설정을 저장하려면 **적용**을 클릭합니다.

Password Manager 인증 구성

Password Manager 페이지에서 사용자가 Password Manager에 인증하는 방법을 구성할 수 있습니다.

Password Manager 인증 구성 방법:

왼쪽 창의 인증에서 **Password Manager**를 선택합니다.

설정하려는 역할을 선택하려면 **로그인 옵션 적용 대상** 목록에서 **사용자** 또는 **관리자**를 선택합니다. 이 페이지의 변경 사항은 모두 선택한 역할에만 적용됩니다.

(선택사항) **인증을 요구하지 않음** 확인란을 선택하면 선택된 사용자 역할이 Password Manager에 저장된 자격 증명을 통해 모든 소프트웨어 응용 프로그램 및 인터넷 웹사이트에 자동 로그인됩니다.

인증 시 사용 가능한 옵션을 설정합니다.

기본적으로 각각의 인증 방법은 다른 인증 방법과 함께 사용하지 않고 개별적으로 사용하도록 구성되어 있습니다. 다음과 같은 방법으로 기본값을 변경할 수 있습니다.

인증 옵션의 조합을 설정하려면 사용 가능한 옵션 아래에서 ⁄을 클릭하여 첫 번째 인증 방법을 선택합니다. 사용 가능한 옵션 대화 상자에서 두 번째 인증 방법을 선택하고 **확인**을 클릭합니다.

예를 들어, 로그온 자격 증명으로 지문과 암호를 모두 요청할 수 있습니다. 대화 상자에서, 지문 인증을 통해 사용해야 하는 두 번째 인증 방법을 선택합니다.

각 인증 방법을 개별적으로 사용할 수 있도록 하려면 사용 가능한 옵션 대화 상자에서 두 번째 인증 방법을 **적용 안 함**으로 설정된 채로 두고 **확인**을 클릭합니다.

로그인 옵션을 제거하려면 사용 가능한 옵션의 로그인 옵션 페이지에서 **X**를 클릭하고 인증 방식을 제거할 수 있습니다.

새로운 조합의 인증 방식을 추가하려면 **옵션 추가**를 클릭합니다.

선택한 역할의 설정을 저장하려면 **적용**을 클릭합니다.

 : **기본값 단추를 선택하면 설정이 초기 값으로 복구됩니다.**

복구 질문 구성

복구 질문 페이지에서는 개인적인 복구 질문 및 답변을 정의할 때 사용자에게 나타나는 질문을 선택할 수 있습니다. 사용자는 암호가 만료되었거나 암호를 잊었을 때 이 복구 질문을 이용해 컴퓨터에 대한 액세스 권한을 복구할 수 있습니다.

복구 질문 구성 방법:

왼쪽 창의 인증에서 **복구 질문**을 선택합니다.

복구 질문 페이지에서 사전 정의된 복구 질문을 3개 이상 선택합니다.

옵션으로, 사용자가 선택할 수 있는 사용자 지정 질문을 최대 3개까지 목록에 추가할 수 있습니다.

복구 질문을 저장하려면 **적용**을 클릭합니다.

지문 스캔 인증 구성

지문 스캔 인증 구성 방법:

왼쪽 창의 인증 아래에서 **지문**을 선택합니다.

등록에서 사용자가 등록할 수 있는 최소 및 최대 지문 개수를 설정합니다.

지문 스캔 민감도를 설정합니다.

민감도가 낮을수록 잘못된 스캔을 수락할 가능성과 허용 편차가 증가합니다. 가장 높게 설정하면 올바른 지문이 거부될 수도 있습니다. 민감도가 높을수록 타인 수락 오류율이 1/10,000로 낮아집니다.

지문 판독기의 버퍼에서 모든 지문 스캔과 자격 증명 등록을 제거하려면 **판독기 지우기**를 클릭합니다. 이때 데이터는 현재 추가한 데이터만 제거되고, 이전 세션에서 저장한 스캔과 등록은 삭제되지 않습니다.

설정을 저장하려면 **적용**을 클릭합니다.

OTP(일회용 암호) 인증 구성

: OTP(일회용 암호) 기능을 사용하려면 TPM을 설치하고, 활성화해야 하며, 소유권을 가지고 있어야 합니다. TPM 설정에 대한 지침은 일회용 암호에 대한 사전 설치 구성을 참조하십시오.

일회용 암호 기능을 사용하려면 사용자가 모바일 장치에서 Security Tools Mobile 앱을 사용하여 일회용 암호를 생성하고 컴퓨터에 해당 암호를 입력합니다. 암호는 한 번만 사용할 수 있으며 제한된 기간 동안에만 유효합니다.

관리자가 보안을 더욱 강화하려면 암호를 요청하여 모바일 응용 프로그램의 안전 여부를 확인할 수 있습니다.

모바일 장치 및 OTP의 보안 강화는 모바일 장치 페이지에서 설정을 구성하면 가능합니다.

OTP 인증 구성 방법:

왼쪽 창의 인증에서 **모바일 장치**를 선택합니다.

사용자에게 모바일 장치에서 암호를 입력하여 Security Tools Mobile 앱에 액세스하도록 요청하려면 **암호 필요**를 선택합니다.

: 모바일 장치를 컴퓨터에 등록한 후에 *암호 필요* 정책을 활성화하면 모든 모바일 장치의 등록이 해제됩니다. 이 정책이 활성화되면 모바일 장치를 다시 등록하라는 메시지가 표시됩니다.

암호 필요 확인란이 선택되어 있으면 사용자가 모바일 장치의 잠금을 해제해야 Security Tools Mobile 앱에 액세스할 수 있습니다. 장치 잠금이 모바일 장치에 표시되지 않더라도 암호를 요구하게 됩니다.

OTP(일회용 암호) 길이를 선택하려면 **일회용 암호 길이**에서 요구할 암호 문자 수를 선택합니다.

사용자가 OTP를 정확히 입력해야 하는 횟수를 선택하려면 **허용되는 사용자 로그인 시도**에서 **5~30**까지 숫자 하나를 선택합니다.

최대 횟수에 도달한 경우 OTP 기능은 사용자가 모바일 장치를 다시 등록할 때까지 사용할 수 없습니다.

: OTP 외에 인증 방식을 한 가지 이상 추가로 설정하는 것이 좋습니다.

스마트 카드 등록 구성

DDP|Security Tools는 비접촉식과 접촉식, 두 가지 방식의 스마트 카드를 지원합니다.

접촉식 카드는 카드를 삽입할 스마트 카드 판독기가 필요하며, 도메인 컴퓨터와만 호환됩니다. CAC 및 SIPRNet 카드는 모두 접촉식입니다. 이 카드는 고급 특성상 사용자가 카드를 삽입하여 로그온한 후 인증서를 선택해야 합니다.

비접촉식 카드는 비도메인 컴퓨터 및 도메인 사양으로 구성된 컴퓨터에서 지원됩니다.

사용자는 사용자 계정 하나당 접촉식 스마트 카드 1개, 혹은 비접촉식 카드 여러 개를 등록할 수 있습니다.

부팅 전 인증에서는 스마트 카드가 지원되지 않습니다.

: 다수의 카드가 등록된 계정에서 1개의 스마트 카드 등록을 제거할 경우 모든 카드가 동시에 등록 해제됩니다.

스마트 카드 등록 구성 방법:

관리자 설정 도구의 인증 탭에서 **스마트 카드**를 선택합니다.

고급 권한 구성

고급 최종 사용자 옵션을 수정하려면 **고급**을 클릭합니다. *고급* 아래에서 필요에 따라 사용자가 자격 증명을 직접 등록하고 등록된 자격 증명을 수정하여 원스텝 로그온을 수행할 수 있도록 허용할 수 있습니다.

다음 확인란을 선택하거나 지웁니다.

사용자의 자격 증명 등록 허용 - 기본적으로 확인란이 선택되어 있습니다. 사용자가 관리자의 개입 없이 자격 증명을 등록할 수 있습니다. 확인란을 지울 경우 관리자가 자격 증명을 등록해야 합니다.

사용자의 등록된 자격 증명 수정 허용 - 기본적으로 확인란이 선택되어 있습니다. 선택되어 있으면 사용자가 관리자의 개입 없이 등록된 자격 증명을 수정하거나 삭제할 수 있습니다. 확인란을 지울 경우 자격 증명을 일반 사용자가 수정하거나 삭제할 수 없으며, 관리자가 수정하거나 삭제해야 합니다.

: 사용자의 자격 증명을 등록하려면 관리자 설정 도구의 *사용자* 페이지로 이동하여 사용자를 선택하고 등록을 클릭합니다.

원스텝 로그온 허용 - 원스텝 로그온이란 SSO(Single Sign-on)를 말합니다. 확인란이 기본적으로 선택되어 있습니다. 이 기능을 활성화할 경우 사용자는 부팅 전 인증 화면에서만 자격 증명을 입력하면 됩니다. 사용자가 Windows에 자동으로 로그온됩니다. 이 확인란을 선택 취소하면 여러 차례 로그온해야 할 수도 있습니다.

: 이 옵션은 사용자의 자격 증명 등록 허용 설정도 선택되어 있어야 사용할 수 있습니다.

완료되면 **적용**을 클릭합니다.

사용자 인증 관리

관리자 설정 인증 탭의 컨트롤은 사용자 로그온 옵션을 설정하거나 각 옵션 설정을 사용자 지정하는 데 사용됩니다.

사용자 인증 관리 방법:

1 관리자 권한으로 **관리자 설정** 타일을 클릭합니다.

2 **사용자** 탭을 클릭하고 사용자를 관리하거나 사용자 등록 상태를 확인합니다. 이 탭의 기능은 다음과 같습니다.

- 새로운 사용자 등록
- 자격 증명 추가 또는 변경
- 사용자의 자격 증명 제거

노트:
로그인 및 **세션**에 사용자의 등록 상태가 표시됩니다.

로그인 상태가 **정상**이면 사용자가 로그온하는 데 필요한 모든 등록이 완료된 것입니다. **세션** 상태가 **정상**이면 사용자가 Password Manager를 사용하는 데 필요한 모든 등록이 완료된 것입니다.

둘 중 하나의 상태가 **미완료**이면 사용자가 추가 등록을 완료해야 합니다. 필요한 등록을 확인하려면 **관리자 설정** 도구를 선택하고 **사용자** 탭을 엽니다. 회색 확인 표시 상자는 완료되지 않은 등록을 나타냅니다. 또는 **등록** 타일을 클릭하고 **상태** 탭의 **정책** 열에서 나열된 필요한 등록을 검토합니다.

새 사용자 추가

: 새 Windows 사용자가 Windows에 로그인하거나 자격 증명을 등록하면 자동으로 추가됩니다.

기존 Windows 사용자의 등록 프로세스를 시작하려면 **사용자 추가**를 클릭합니다.
사용자 선택 대화 상자가 표시되면 **개체 유형**을 선택합니다.
텍스트 상자에 사용자의 개체 이름을 입력하고 **이름 확인**을 클릭합니다.
모두 마쳤으면 **확인**을 클릭합니다.
등록 마법사가 열립니다.

지침에 대한 사용자 자격 증명을 등록하거나 변경으로 계속합니다.

사용자 자격 증명 등록 또는 변경

관리자가 사용자를 대신하여 사용자의 자격 증명을 등록하거나 변경할 수 있지만, 복구 질문에 대답 및 사용자의 지문 스캔과 같은 몇 가지 등록 작업은 사용자가 있어야 합니다.

사용자 자격 증명을 등록하거나 변경하려면 다음을 수행합니다.

관리자 설정에서 **사용자** 탭을 클릭합니다.
사용자 페이지에서 **등록**을 클릭합니다.
시작 페이지에서, **다음**을 클릭합니다.
인증 필요 대화 상자에서 사용자의 Windows 암호를 사용하여 로그인하고 **확인**을 클릭합니다.
암호 페이지에서 사용자의 Windows 암호를 변경하려면 새 암호를 입력한 후 확인하고 **다음**을 클릭합니다.
암호 변경을 건너뛰려면 **건너뛰기**를 클릭합니다. 등록을 원하지 않을 때는 마법사에서 자격 증명을 건너뛸 수 있습니다. 페이지로 돌아가려면 **뒤로**를 클릭합니다.
각 페이지의 지침을 수행하고 **다음**, **건너뛰기**, 또는 **뒤로** 중 적절한 단추를 클릭합니다.
요약 페이지에서 등록된 자격 증명을 확인한 후 등록을 모두 마쳤으면 **적용**을 클릭합니다.
자격 증명 등록 페이지로 돌아가서 정보를 변경하려면 원하는 페이지에 이를 때까지 **뒤로**를 클릭합니다.

자격 증명 등록 또는 변경에 대한 자세한 내용은 *Console 사용 설명서*를 참조하십시오.

등록된 자격 증명 1개 제거

관리자 설정 타일을 클릭합니다.
사용자 탭을 클릭하고 변경할 사용자를 찾습니다.
제거할 자격 증명의 녹색 확인 표시 위로 마우스를 이동합니다. ⊗로 변경됩니다.

- 기호를 클릭하고 **예**를 클릭하여 삭제를 확인합니다.

: 사용자가 등록한 자격 증명이 하나인 경우에는 이러한 방식으로 자격 증명을 제거할 수 없습니다. 또한 이 방법으로 암호를 제거할 수 없습니다. 컴퓨터에 대한 사용자의 액세스 권한을 완전히 제거하려면 제거 명령을 사용하십시오.

사용자의 등록된 자격 증명 모두 제거

관리자 설정 타일을 클릭합니다.
사용자 탭을 클릭하고 제거할 사용자를 찾습니다.
제거를 클릭합니다. (사용자의 설정값 아래쪽에 제거 명령이 빨간색으로 표시됨)
제거되면 사용자가 다시 등록할 때까지 컴퓨터에 로그온할 수 없습니다.

마스터 설치 프로그램을 사용하여 설치 제거

- 각 구성 요소를 별도로 설치 제거한 후에 마스터 설치 프로그램을 설치 제거해야 합니다. **설치 제거 장애를 방지하려면 특정 순서대로** 클라이언트를 설치 제거해야 합니다.
- 하위 설치 프로그램을 가져오려면 마스터 설치 프로그램에서 하위 설치 프로그램 추출의 지침을 따릅니다.
- 설치 작업과 설치 제거 작업에 동일한 버전의 마스터 설치 프로그램(및 해당 클라이언트)을 사용해야 합니다.
- 이 장에서는 하위 설치 프로그램 사용 방법에 대한 *자세한* 지침이 있는 다른 장에 대해 설명합니다. 이 장에서는 마지막 단계인 마스터 설치 프로그램 설치 제거에 **대해서만** 설명합니다.

클라이언트를 다음 순서로 설치 제거합니다.

1 Encryption 클라이언트 설치 제거.
2 Client Security Framework 설치 제거.
3 Advanced Authentication 설치 제거.

드라이버 패키지는 설치 제거할 필요가 없습니다.

설치 제거 방법 선택으로 진행합니다.

설치 제거 방법 선택

마스터 설치 프로그램을 제거하는 방법은 두 가지입니다. 다음 중 **하나**를 선택하십시오.

- 프로그램 추가/제거에서 설치 제거
- 명령줄을 사용하여 설치 제거

프로그램 추가/제거에서 설치 제거

Windows 제어판의 프로그램 제거로 이동합니다(**시작** > **제어판** > **프로그램 및 기능** > **프로그램 제거**).
Dell Data Protection 설치 프로그램을 강조 표시하고 **변경**을 마우스 왼쪽 버튼으로 클릭하여 설정 마법사를 시작합니다.
시작 화면을 읽고 **다음**을 클릭합니다.
프롬프트에 따라 설치를 제거하고 **마침**을 클릭합니다.
컴퓨터를 다시 시작하고 Windows에 로그인합니다.
마스터 설치 프로그램이 설치 제거됩니다.

명령줄을 사용하여 설치 제거

다음 예에서는 마스터 설치 프로그램을 자동으로 설치 제거합니다.

```
"DDPSetup.exe" -y -gm2 /S /x
```

완료되면 컴퓨터를 다시 부팅합니다.

마스터 설치 프로그램이 설치 제거됩니다.

하위 설치 프로그램을 사용하여 설치 제거로 진행합니다.

8

하위 설치 프로그램을 사용하여 설치 제거

- 로컬 또는 도메인 관리자만 암호 해독 및 설치 제거를 수행할 수 있습니다. 명령줄로 설치 제거하는 경우에는 도메인 관리자 자격 증명이 필요합니다.
- 마스터 설치 프로그램으로 Personal Edition을 설치한 경우에는 마스터 설치 프로그램에서 하위 실행 파일 추출에 설명된 대로 설치 제거 전에 마스터 설치 프로그램에서 하위 실행 파일을 추출해야 합니다.
- 설치 작업과 설치 제거 작업에 동일한 버전의 클라이언트를 사용해야 합니다.
- 가능하면 야간에 암호 해독을 실행할 수 있도록 계획하십시오.
- 사용자가 없는 시간에 컴퓨터가 절전 모드로 전환되지 않도록 절전 모드를 해제하십시오. 절전 중인 컴퓨터에서는 암호 해독이 실행되지 않습니다.
- 잠긴 파일로 인한 실패를 최소화하기 위해 모든 프로세스와 응용 프로그램을 종료합니다.

Encryption 클라이언트 설치 제거

- **설치 제거 프로세스를 시작하기 전에** (선택 사항) Encryption Removal Agent 로그 파일을 생성할 수 있습니다. 이 로그 파일은 설치 제거/암호 해독 작업의 문제를 해결하는 데 유용합니다. 설치 제거 프로세스 중 파일을 암호 해독하지 않으려면 Encryption Removal Agent 로그 파일을 만들지 않아도 됩니다.
- 설치 제거가 완료된 후, 컴퓨터를 다시 시작하기 전에 모든 데이터가 암호 해독되도록 하려면 WSScan를 실행하십시오. 지침은 WSScan 사용을 참조하십시오.
- 정기적으로 Encryption Removal Agent 상태 확인 서비스 패널에 Encryption Removal Agent 서비스가 여전히 있는 경우에 데이터 암호 해독이 계속 진행 중입니다.

설치 제거 방법 선택

Encryption 클라이언트를 제거하는 방법은 두 가지입니다. 다음 중 **하나**를 선택하십시오.

사용자 인터페이스를 사용하여 설치 제거
명령줄을 사용하여 설치 제거

사용자 인터페이스를 사용하여 설치 제거

Windows 제어판의 프로그램 제거로 이동합니다(**시작** > **제어판** > **프로그램 및 기능** > **프로그램 제거**).
Encryption을 강조 표시하고 **변경**을 마우스 왼쪽 버튼으로 클릭하여 Personal Edition 설정 마법사를 시작합니다.
시작 화면을 읽고 **다음**을 클릭합니다.
Encryption Removal Agent 설치 화면에서 다음 중 하나를 선택합니다.

: 두 번째 옵션은 기본적으로 활성화되어 있습니다. 파일을 암호 해독하려면 선택 항목을 첫 번째 옵션으로 변경해야 합니다.

Encryption Removal Agent - 파일에서 키 가져오기

SDE, 사용자 또는 일반 암호화의 경우 이 옵션은 파일을 암호 해독하고 Encryption 클라이언트를 설치 제거합니다. ***이는 권장되는 선택입니다.***

Encryption Removal Agent 설치 안 함

이 옵션은 Encryption 클라이언트를 설치 제거하지만 *파일을 암호 해독하지 않습니다*. 이 옵션은 Dell ProSupport의 지시에 따라 문제 해결 목적을 **위해서만** 사용해야 합니다.

다음을 클릭합니다.

백업 파일 텍스트 상자에 백업 파일의 네트워크 드라이브 또는 이동식 매체 위치의 경로를 입력하거나 **...**를 클릭하고 위치를 찾아봅니다. 파일 형식은 LSARecovery_[hostname].exe입니다.

암호 텍스트 상자에 암호화 관리자 암호를 입력합니다. 이것은 소프트웨어를 설치할 때 설정 마법사에서 설정한 암호입니다.

다음을 클릭합니다.

Dell Decryption Agent 서비스 로그온 이름 화면에 두 가지 옵션이 있습니다. **로컬 시스템 계정**을 선택합니다. **마침**을 클릭합니다.

프로그램 제거 화면에서 **제거**를 클릭합니다.

구성 완료 화면에서 **마침**을 클릭합니다.

컴퓨터를 다시 시작하고 Windows에 로그온합니다.

암호 해독이 진행 중입니다.

암호 해독 프로세스는 암호 해독 중인 드라이브의 수 및 해당 드라이브에 있는 데이터의 양에 따라 몇 시간까지 소요될 수 있습니다. 암호 해독 프로세스를 확인하려면 Encryption Removal Agent 상태 확인을 참조하십시오.

명령줄을 사용하여 설치 제거

명령줄 스위치 및 매개 변수는 대/소문자를 구분합니다.

명령줄에서 공백과 같은 특수 문자를 하나 이상 포함하는 값은 이스케이프된 따옴표로 묶어야 합니다. 명령줄 매개 변수는 대/소문자를 구분합니다.

이러한 설치 프로그램을 사용하여 스크립팅된 설치, 배치 파일 또는 조직에 제공되는 다른 푸시 기술을 통해 클라이언트를 설치 제거합니다.

로그 파일

Windows는 로그인된 사용자에 대해 고유한 하위 설치 프로그램 설치 제거 로그 파일을 C:\Users\<UserName>\AppData\Local\Temp의 %temp%에 생성합니다.

설치 프로그램을 실행할 때 별도의 로그 파일을 추가하려는 경우, 하위 설치 프로그램이 첨부되지 않으므로 해당 로그 파일의 이름은 고유해야 합니다. 표준 .msi 명령을 통해 /l C:\<any directory>\<any log file name>.log를 사용하여 로그 파일을 생성할 수 있습니다. 명령줄 설치 제거에서는 사용자 이름/암호가 로그 파일에 기록되므로 "/l*v"(자세한 로깅)를 사용하지 않는 것이 좋습니다.

별도로 표시된 경우를 제외하고, 모든 하위 설치 프로그램은 명령줄 설치 제거에 동일한 기본 .msi 스위치와 표시 옵션을 사용합니다. 스위치를 먼저 지정해야 합니다. /v 스위치가 필요하며 인수를 사용합니다. 다른 매개 변수는 인수 안에 포함되어 /v 스위치로 전달됩니다.

표시 옵션은 예상 동작을 수행하도록 /v 스위치에 전달된 인수 끝에 지정할 수 있습니다. 동일한 명령줄에 /q와 /qn을 동시에 사용하지 마십시오. /qb 이후에 ! 및 - 만 사용합니다.

스위치	의미
/v	변수를 setup.exe 안의 .msi로 전달
/s	자동 모드
/x	설치 제거 모드

옵션	의미
/q	진행률 대화 상자가 없습니다. 프로세스 완료 후 자동으로 다시 시작합니다.
/qb	**취소** 단추가 있는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/qb-	**취소** 단추가 있는 진행률 대화 상자로, 프로세스 완료 후 자동으로 다시 시작합니다.

옵션	의미
/qb!	**취소** 단추가 없는 진행률 대화 상자로, 다시 시작할 것인지 묻습니다.
/qb!-	**취소** 단추가 없는 진행률 대화 상자로, 프로세스 완료 후 자동으로 다시 시작합니다.
/qn	사용자 인터페이스 없음

마스터 설치 프로그램에서 추출된 후에 Encryption 클라이언트 설치 프로그램은 C:\extracted\Encryption\DDPE_XXbit_setup.exe에서 찾을 수 있습니다.

다음 표에는 설치 제거 시 사용할 수 있는 매개 변수가 나와 있습니다.

매개변수	선택
CMG_DECRYPT	Encryption Removal Agent 설치 유형 선택 속성: 2 - Forensic 키 번들을 사용하여 키 가져 오기 0 - Encryption Removal Agent를 설치하지 않음
CMGSILENTMODE	자동 설치 제거 속성: 1 - 자동 0 - 수동
DA_KM_PW	도메인 관리자 계정의 암호.
DA_KM_PATH	키 자료 번들 경로.

다음 예에서는 Encryption Removal Agent를 설치하지 않고 Encryption 클라이언트를 설치 제거합니다.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=0 CMGSILENTMODE=1 DA_KM_PATH=C:\FullPathToLSA.exe
DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

다음 예에서는 Forensic 키 번들을 사용하여 Encryption 클라이언트를 설치 제거합니다. Forensic 키 번들을 로컬 디스크에 복사하고 다음 명령을 실행합니다.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENTMODE=1 DA_KM_PATH=C:
\FullPathToForensicKeyBundle DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

완료되면 컴퓨터를 다시 부팅합니다.

암호 해독 프로세스는 암호 해독 중인 드라이브의 수 및 해당 드라이브에 있는 데이터의 양에 따라 몇 시간까지 소요될 수 있습니다. 암호 해독 프로세스를 확인하려면 Encryption Removal Agent 상태 확인을 참조하십시오.

Advanced Authentication 설치 제거

설치 제거 방법 선택

Encryption 클라이언트를 제거하는 방법은 두 가지입니다. 다음 중 **하나**를 선택하십시오.

사용자 인터페이스를 사용하여 설치 제거
명령줄을 사용하여 설치 제거

사용자 인터페이스를 사용하여 설치 제거

Windows 제어판의 프로그램 제거로 이동합니다(**시작** > **제어판** > **프로그램 및 기능** > **프로그램 제거**).

Security Tools Authentication을 강조 표시하고 **변경**을 마우스 왼쪽 단추로 클릭하여 설정 마법사를 시작합니다.

시작 화면을 읽고 **다음**을 클릭합니다.
관리자 암호를 입력합니다.
프롬프트에 따라 설치를 제거하고 **마침**을 클릭합니다.
컴퓨터를 다시 시작하고 Windows에 로그인합니다.

Security Tools Authentication이 설치 제거됩니다.

명령줄을 사용하여 설치 제거

마스터 설치 프로그램에서 추출된 후에 Advanced Authentication 클라이언트 설치 프로그램은 **C:\extracted\Security Tools\Authentication\<x64/x86>\setup.exe**에서 찾을 수 있습니다.
다음 예에서는 Advanced Authentication 클라이언트를 자동으로 설치 제거합니다.

```
setup.exe /x /s /v" /qn"
```

완료되면 컴퓨터를 종료하고 다시 시작합니다.

정책 및 템플릿 설명으로 진행합니다.

Client Security Framework 설치 제거

설치 제거 방법 선택

Encryption 클라이언트를 제거하는 방법은 두 가지입니다. 다음 중 **하나**를 선택하십시오.

사용자 인터페이스를 사용하여 설치 제거
명령줄을 사용하여 설치 제거

사용자 인터페이스를 사용하여 설치 제거

Windows 제어판의 프로그램 제거로 이동합니다(**시작** > **제어판** > **프로그램 및 기능** > **프로그램 제거**).
Client Security Framework를 강조 표시하고 **변경**을 마우스 왼쪽 버튼으로 클릭하여 설정 마법사를 시작합니다.
시작 화면을 읽고 **다음**을 클릭합니다.
프롬프트에 따라 설치를 제거하고 **마침**을 클릭합니다.
컴퓨터를 다시 시작하고 Windows에 로그온합니다.

Client Security Framework가 설치 제거됩니다.

명령줄을 사용하여 설치 제거

마스터 설치 프로그램에서 추출된 후에 Client Security Framework 클라이언트 설치 프로그램은 에서 찾을 수 있습니다. **C:\extracted\Security Tools\EMAgent_**.
다음 예에서는 SED 클라이언트를 자동으로 설치 제거합니다.

```
EMAgent_XXbit_setup.exe /x /s /v" /qn"
```

완료되면 컴퓨터를 종료하고 다시 시작합니다.

정책 및 템플릿 설명

로컬 관리 콘솔의 정책 위에 마우스를 올려 놓으면 도구 설명이 표시됩니다.

정책

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
고정 저장소 정책										
SDE 암호화 사용	참								거짓	이 정책은 다른 모든 SDE(System Data Encryption) 정책의 "마스터 정책"입니다. 이 정책이 "거짓"이면 다른 정책 값에 관계없이 SDE 암호화가 발생하지 않습니다. "참"이면 다른 지능형 암호화 정책으로 암호화되지 않은 모든 데이터가 SDE 암호화 규칙 정책에 따라 암호화됩니다. 이 정책 값을 변경하면 재부팅해야 합니다.
SDE 암호화 알고리즘	AES256									AES 256, AES 128, 3DES
SDE 암호화 규칙										특정 드라이브, 디렉터리 및 폴더를 암호화/암호화하지 않는 데 사용할 암호화 규칙입니다. 기본값 변경에 대해 잘 모를 경우 도움을 받으려면 Dell ProSupport에 문의하십시오.
일반 설정 정책										
암호화 사용	참							거짓		이 정책은 모든 일반 설정 정책의 "마스터 정책"입니다. "거짓"이면 다른 정책 값에 관계없이 암호화가 발생하지 않습니다.

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
										"참"이면 모든 암호화 정책이 사용됩니다. 이 정책 값을 변경하면 새 스윕이 트리거되어 파일을 암호화/암호 해독합니다.
일반 암호화된 폴더										문자열 - 각각 500자로 구성된 최대 100개 항목(최대 2048자) 암호화 또는 암호화 제외 대상인 끝점 드라이브의 폴더 목록으로, 끝점에 액세스할 수 있는 모든 관리되는 사용자가 액세스할 수 있습니다. 사용 가능한 드라이브 문자는 다음과 같습니다. #: 모든 드라이브 f#: 모든 고정 드라이브 r#: 모든 이동식 드라이브 중요: 디렉터리 보호를 재정의하면 컴퓨터를 부팅할 수 없고 드라이브를 재포맷해야 할 수 있습니다. 같은 폴더가 이 정책과 사용자 암호화 폴더 정책에 모두 지정된 경우에는 이 정책이 우선 적용됩니다.
일반 암호화 알고리즘	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES 시스템 페이징 파일은 AES 128을 사용하여 암호화됩니다.
Application Data Encryption 목록	winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe									문자열 - 각각 500자로 구성된 최대 100개 항목 예기치 않았거나 의도하지 않은 결과가 발생할 수 있으므로 explorer.exe 또는 iexplorer.exe를 ADE 목록에 추가하지 않는 것이 좋습니다. 하지만 explorer.exe는 마우스 오른쪽 버튼 클릭 메뉴를 통해 데스크톱에서 새 메모장 파일을 만드는 프로세스로 사용할 수 있습니다. ADE 목록 대신 파일 확장명으로 암호화

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
	visio.exe mspub.exe notepad.exe wordpad.exe winzip.exe winrar.exe onenote.exe onenotem.exe									를 설정하면 더욱 포괄적인 적용 범위가 가능해집니다. 새 파일을 암호화할 응용 프로그램의 프로세스 이름 목록(경로 제외)을 나열하며, 캐리지 리턴으로 구분합니다. 와일드카드를 사용하지 마십시오. Dell 권장 사항에 따라 시스템에 중요한 파일을 작성하는 응용 프로그램/설치 프로그램을 나열하지 않는 것이 좋습니다. 이렇게 하면 중요한 시스템 파일이 암호화되어 컴퓨터를 부팅할 수 없게 됩니다. 일반 프로세스 이름: outlook.exe, winword.exe, frontpg.exe, powerpnt.exe, msaccess.exe, wordpad.exe, mspaint.exe, excel.exe 다음 하드 코딩된 시스템 및 설치 프로그램 프로세스 이름은 이 정책에 지정된 경우 무시됩니다. hotfix.exe, update.exe, setup.exe, msiexec.exe, wuauclt.exe, wmiprvse.exe, migrate.exe, unregmp2.exe, ikernel.exe, wssetup.exe, svchost.exe
Application Data Encryption 키	일반									일반 또는 사용자 Application Data Encryption 목록에 따라 암호화된 파일에 액세스할 수 있는 사람 및 액세스 위치를 나타내는 키를 선택합니다. 일반 - 파일이 생성된 끝점에서, 관리되는 모든 사용자가 이러한 파일에 액세스하고(일반 암호화된 폴더와 같은 액세스 수준) 일반 암호화 알고리즘으로 이 파일을 암호화할 수 있도록 하려는 경우 선택합니다. 사용자 - 오직 파일이 생성된 끝점에서, 파일을 만든 사용자만 이러한 파일에 액세스하

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
										고(사용자가 암호화한 폴더와 같은 액세스 수준) 사용자 암호화 알고리즘으로 이 파일을 암호화할 수 있도록 하려는 경우 선택합니다. 이 정책에 대한 변경 사항은 이 정책 때문에 이미 암호화된 파일에는 영향을 주지 않습니다.
Outlook 개인 폴더 암호화	참							거짓		"참"이면 Outlook 개인 폴더를 암호화합니다.
임시 파일 암호화	참							거짓		"참"이면 User Data Encryption 키로 환경 변수 TEMP 및 TMP에 나열된 경로를 암호화합니다.
임시 인터넷 파일 암호화	참	거짓								"참"이면 User Data Encryption 키를 사용하여 환경 변수 CSIDL_INTERNET_CACHE에 나열된 경로를 암호화합니다. 암호화 스윕 시간을 줄이기 위해 클라이언트가 초기 암호화에 대한 CSIDL_INTERNET_CACHE 내용 및 이 정책 관련 업데이트를 지웁니다. Microsoft Internet Explorer를 사용하는 경우에만 이 정책을 적용할 수 있습니다.
사용자 프로필 문서 암호화	참								거짓	"참"이면 다음을 암호화합니다. · 사용자 데이터 암호화 키가 포함된 사용자 프로필(C:\Users\jsmith) · 일반 암호화 키가 포함된 \Users\Public
Windows 페이징 파일 암호화	참								거짓	"참"으로 설정하면 Windows 페이징 파일이 암호화됩니다. 이 정책을 변경하면 재부팅을 해야 합니다.
관리되는 서비스										문자열 - 각각 500자로 구성된 최대 100개 항목(최대 2048자)

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
										이 정책에 의해 관리되는 서비스는 사용자가 로그인하고 클라이언트가 잠금 해제된 후에만 시작됩니다. 이 정책은 또한 이 정책에 의해 관리되는 서비스가 로그오프 도중 클라이언트가 잠기기 전에 중지되도록 합니다. 이 정책은 서비스가 응답하지 않는 경우 사용자 로그오프를 방지하기도 합니다. 구문은 라인별 서비스 이름입니다. 서비스 이름에 공백을 사용할 수 있습니다. 와일드카드는 사용할 수 없습니다. 관리되지 않는 사용자가 로그온하면 관리되는 서비스가 시작되지 않습니다.
보안 암호화 후처리	3단계 덮어쓰기	1단계 덮어쓰기							덮어쓰기 없음	덮어쓰기 없음, 1단계 덮어쓰기, 3단계 덮어쓰기, 7단계 덮어쓰기 이 범주의 다른 정책을 통해 지정된 폴더가 암호화되면 이 정책은 원본 파일 중 암호화되지 않은 나머지 부분을 처리하는 방법을 결정합니다. · 덮어쓰기 없음을 사용하면 나머지 부분을 삭제합니다. 이 값을 사용하면 암호화 처리 속도가 가장 빨라집니다. · 1단계 덮어쓰기를 사용하면 나머지 부분을 임의 데이터로 덮어씁니다. · 3단계 덮어쓰기를 사용하면 나머지 부분을 1s 및 0s의 표준 패턴, 해당 보집합, 임의 데이터 순으로 덮어씁니다. · 7단계 덮어쓰기를 사용하면 나머지 부분을 1s 및 0s의 표준 패턴, 해당 보집합, 임의 데이터 5회 순으로 덮어씁니다. 이 값을 사용하면 메모리에서 원본 파일 복구가 가장 어렵고 가장 안전하게 암호화가 처리됩니다.
Windows 최대 절전	참					거짓		참	거짓	사용하도록 설정하면 컴퓨터가 최대 절전 모드로 전환될

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
모드 파일 보안										경우에만 최대 절전 모드 파일이 암호화됩니다. 컴퓨터가 최대 절전 모드에서 나오면 클라이언트가 보호를 풀어 컴퓨터가 사용 중인 동안 사용자나 응용 프로그램에 영향을 미치지 않고 컴퓨터를 보호합니다.
비보안 최대 절전 모드 방지	참					거짓		참	거짓	사용하도록 설정하면 클라이언트가 최대 절전 모드 데이터를 암호화할 수 없을 경우 컴퓨터 최대 절전 모드를 허용하지 않습니다.
워크스테이션 스캔 우선 순위	높음	보통								가장 높음, 높음, 보통, 낮음, 가장 낮음 암호화된 폴더 스캔의 상대적 Windows 우선 순위를 지정합니다.
사용자가 암호화한 폴더										문자열 - 각각 500자로 구성된 최대 100개 항목(최대 2048자) User Data Encryption 키로 암호화하거나 암호화에서 제외할 끝점 하드 드라이브의 폴더 목록입니다. 이 정책은 Windows에서 하드 디스크 드라이브로 분류된 모든 드라이브에 적용됩니다. 이 정책은 유형이 이동식 디스크로 표시되는 드라이브나 외부 미디어를 암호화하는 데 사용할 수 없습니다. EMS 외부 미디어 암호화를 대신 사용하십시오.
사용자 암호화 알고리즘	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES 개별 사용자 수준에서 데이터를 암호화하는 데 사용된 암호화 알고리즘입니다. 동일한 끝점을 사용하는 다른 사용자에 대해 서로 다른 값을 지정할 수 있습니다.
User Data Encryption 키	사용자	일반		사용자	일반				사용자	일반 또는 사용자 다음 정책에 따라 암호화된 파일에 액세스할 수 있는 사람 및 액세스 위치를 나타내는 키를 선택합니다.

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
										· 사용자가 암호화한 폴더 · Outlook 개인 폴더 암호화 · 임시 파일 암호화 (\Documents and Settings \username\Local Settings \Temp만 해당) · 임시 인터넷 파일 암호화 · 사용자 프로필 문서 암호화 다음을 선택합니다. · 일반 - 사용자가 암호화한 파일/폴더가 생성된 끝점에서, 관리되는 모든 사용자가 이러한 파일/폴더에 액세스하고(일반 암호화된 폴더와 같은 액세스 수준) 일반 암호화 알고리즘으로 이 파일/폴더를 암호화할 수 있도록 하려는 경우 선택합니다. · 사용자 - 오직 파일이 생성된 끝점에서, 파일을 만든 사용자만 이러한 파일에 액세스하고(사용자가 암호화한 폴더와 같은 액세스 수준) 사용자 암호화 알고리즘으로 이 파일을 암호화할 수 있도록 하려는 경우 선택합니다. 전체 디스크 파티션을 암호화하기 위해 암호화 정책을 통합하도록 선택한 경우에는 일반이나 사용자가 아닌 기본 SDE 암호화 정책을 사용하는 것이 좋습니다. 이렇게 하면 관리되는 사용자가 로그인하지 않은 상태일 때 암호화된 운영 체제 파일에 액세스할 수 있습니다.
Hardware Crypto Accelerator(v8.3에서 v8.9.1 Encryption 클라이언트까지만 지원)										
HCA(Hardware Crypto Accelerator)	거짓									이 정책은 다른 모든 HCA(Hardware Crypto Accelerator) 정책의 "마스터 정책"입니다. 이 정책이 "거짓"이면 다른 정책 값에 관계없이 HCA 암호화가 발생하지 않습니다. HCA 정책은 Hardware Crypto Accelerator가 내장된 컴퓨터에서만 사용할 수 있습니다.

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
암호화 대상 볼륨	모든 고정 볼륨									모든 고정 볼륨 또는 시스템 볼륨만 암호화 대상 볼륨을 지정합니다.
HCA로 암호화된 드라이브에 Forensic 메타데이터 사용 가능	거짓									참 또는 거짓 참이면 forensics 메타데이터가 드라이브에 포함되어 Forensic이 간편해집니다. 포함된 메타데이터: • 현재 시스템의 MCID(시스템 ID) • 설치된 현재 Shield의 장치 ID(DCID/SCID) 거짓이면 Forensics 메타데이터가 드라이브에 포함되지 않습니다. "거짓"에서 "참"으로 전환하면 Forensic 추가에 대한 HCA 정책에 따라 다시 스윕됩니다.
보조 드라이브 암호화에 대한 사용자 승인 허용	거짓									"참"으로 설정하면 사용자가 추가 드라이브 암호화 여부를 결정할 수 있습니다.
암호화 알고리즘	AES256									AES 256 또는 AES 128
포트 제어 정책										
포트 제어 시스템	사용 안 함									모든 포트 제어 시스템 정책을 사용하거나 사용하지 않도록 설정합니다. 이 정책을 사용 안 함으로 설정하는 경우 다른 포트 제어 시스템 정책과 상관없이 포트 제어 시스템 정책이 적용되지 않습니다. **참고**: 모든 PCS 정책은 재부팅한 후에 적용됩니다.
포트: Express Card 슬롯	사용									Express Card 슬롯을 통해 노출된 포트를 사용하거나, 사용하지 않거나, 무시합니다.

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
포트: eSATA	사용									외부 SATA 포트에 대한 포트 액세스를 사용하거나, 사용하지 않거나, 무시합니다.
포트: PCMCIA	사용									PCMCIA 포트에 대한 포트 액세스를 사용하거나, 사용하지 않거나, 무시합니다.
포트: Firewire(1394)	사용									외부 Firewire(1394) 포트에 대한 포트 액세스를 사용하거나, 사용하지 않거나, 무시합니다.
포트: SD	사용									SD 카드 포트에 대한 포트 액세스를 사용하거나, 사용하지 않거나, 무시합니다.
하위 클래스 저장소: 외부 드라이브 제어	차단됨	읽기 전용			전체 액세스			읽기 전용	전체 액세스	클래스 하위 항목: 저장소 클래스: 이 정책을 사용하려면 저장소를 "사용"으로 설정해야 합니다. 이 정책은 PCS와 상호 작용합니다. EMS와 PCS 상호 작용을 참조합니다. 전체 액세스: 외부 드라이브 포트에는 읽기/쓰기 데이터 제한이 적용되지 않습니다. 읽기 전용: 읽기 기능이 허용됩니다. 데이터 쓰기를 사용할 수 없습니다. 차단됨: 포트에 읽기/쓰기 기능이 차단됩니다. 이 정책은 끝점을 기반으로 하며 사용자 정책에서 재정의할 수 없습니다.
포트: MTD(메모리 전송 장치)	사용									MTD(메모리 전송 장치) 포트에 대한 액세스를 사용하거나 사용하지 않거나 무시합니다.
클래스: 저장소	사용									다음 3개 정책에 대한 상위 항목입니다. 다음 3개 하위 클래스 저장소 정책을 사용하려면 이 정책을 "사용"으로 설정합니다. 이 정책을 "사용 안 함"으로 설정하면 값과 상관없이 3개 하위 클래스 저장소 정책을 모두 사용할 수 없습니다.

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
하위 클래스 저장소: 광 드라이브 제어	읽기 전용	UDF 전용				전체 액세스		UDF 전용	전체 액세스	클래스 하위 항목: 저장소 클래스: 이 정책을 사용하려면 저장소를 "사용"으로 설정해야 합니다. 전체 액세스: 광 드라이브 포트에는 읽기/쓰기 데이터 제한이 적용되지 않습니다. UDF 전용: UDF 형식이 아닌 모든 데이터 쓰기를 차단합니다(CD/DVD 굽기, ISO 굽기). 데이터 읽기가 사용됩니다. 읽기 전용: 읽기 기능이 허용됩니다. 데이터 쓰기를 사용할 수 없습니다. 차단됨: 포트에 읽기/쓰기 기능이 차단됩니다. 이 정책은 끝점을 기반으로 하며 사용자 정책에서 재정의할 수 없습니다. UDF(범용 디스크 형식)는 ISO/IEC 13346 및 ECMA-167이라고 하는 사양을 구현한 것으로, 광범위한 미디어의 컴퓨터 데이터 저장소에 대한 공개 공급업체 중립 파일 시스템입니다. 이 정책은 PCS와 상호 작용합니다. EMS와 PCS 상호 작용을 참조합니다.
하위 클래스 저장소: 플로피 드라이브 제어	차단됨	읽기 전용				전체 액세스		읽기 전용	전체 액세스	클래스 하위 항목: 저장소 클래스: 이 정책을 사용하려면 저장소를 "사용"으로 설정해야 합니다. 전체 액세스: 플로피 드라이브 포트에는 읽기/쓰기 데이터 제한이 적용되지 않습니다. 읽기 전용: 읽기 기능이 허용됩니다. 데이터 쓰기를 사용할 수 없습니다. 차단됨: 포트에 읽기/쓰기 기능이 차단됩니다. 이 정책은 끝점을 기반으로 하며 사용자 정책에서 재정의할 수 없습니다.

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
클래스: WPD(Windows 휴대용 장치)	사용									다음 정책에 대한 상위입니다. 하위 클래스 WPD(Windows 휴대용 장치): 저장소 정책을 사용하려면 이 정책을 "사용"으로 설정합니다. 이 정책을 "사용 안 함"으로 설정하면 해당 값과 상관없이 하위 클래스 WPD(Windows 휴대용 장치): 저장소 정책을 사용할 수 없습니다. 모든 Windows 휴대용 장치에 대한 액세스를 제어합니다.
하위 클래스 WPD(Windows 휴대용 장치): 저장소	사용									클래스 하위 항목: WPD(Windows 휴대용 장치) 이 정책을 사용하려면 클래스: WPD(Windows 휴대용 장치)를 "사용"으로 설정해야 합니다. 전체 액세스: 포트에는 읽기/쓰기 데이터 제한이 적용되지 않습니다. 읽기 전용: 읽기 기능이 허용됩니다. 데이터 쓰기를 사용할 수 없습니다. 차단됨: 포트에 읽기/쓰기 기능이 차단됩니다.
클래스: HID(휴먼 인터페이스 장치)	사용									모든 휴먼 인터페이스 장치(키보드, 마우스)에 대한 액세스를 제어합니다. **참고**: USB 포트 수준 차단 및 HID 클래스 수준 차단은 컴퓨터 섀시 유형을 랩톱/노트북 폼 팩터로 식별할 수 있는 경우에만 적용됩니다. 섀시 식별에는 컴퓨터 BIOS가 사용됩니다.
클래스: 기타	사용									다른 클래스가 적용되지 않는 모든 장치에 대한 액세스를 제어합니다.
이동식 저장소 정책										
EMS Encrypt External Media(EMS	참					거짓		참	거짓	이 정책은 모든 이동식 저장소 정책의 "마스터 정책"입니다. "거짓"이면 다른 정책 값에 관계없이 이동식 저장소가 암호화되지 않습니다.

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
외부 미디어 암호화)										"참"이면 모든 이동식 저장소 암호화 정책이 적용됩니다. 이 정책은 PCS와 상호 작용합니다. EMS와 PCS 상호 작용을 참조합니다.
EMS CD/DVD 암호화 제외	거짓								참	"거짓"이면 CD/DVD 장치를 암호화합니다. 이 정책은 PCS와 상호 작용합니다. EMS와 PCS 상호 작용을 참조합니다.
EMS Shield로 보호되지 않은 미디어에 대한 EMS 액세스	차단		읽기 전용			전체 액세스		읽기 전용	전체 액세스	차단, 읽기 전용, 전체 액세스 이 정책은 PCS와 상호 작용합니다. EMS와 PCS 상호 작용을 참조합니다. 이 정책을 액세스 차단으로 설정하면 암호화될 때까지 이동식 저장소에 액세스할 수 없습니다. 읽기 전용 또는 전체 액세스를 선택하면 암호화할 이동식 저장소를 결정할 수 있습니다. 이동식 저장소를 암호화하지 않기로 하고 이 정책이 전체 액세스로 설정된 경우에는 이동식 저장소에 대해 전체 읽기/쓰기 권한을 갖습니다. 이동식 저장소를 암호화하지 않을 경우 이 정책이 읽기 전용으로 설정되어 있으면 암호화되지 않은 이동식 저장소에서 기존 파일을 읽거나 삭제할 수 없지만, 암호화되지 않은 이동식 저장소에서 파일을 편집하거나 추가할 수 없습니다.
EMS 암호화 알고리즘	AES256									AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES
EMS 외부 미디어 스캔	참	거짓								"참"이면 이동식 저장소를 삽입할 때마다 EMS에서 이동식 저장소를 스캔할 수 있습니다. 이 정책이 "거짓"이고 EMS 외부 미디어 암호화 정책이

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
										"참"이면 EMS가 새 파일과 변경된 파일만 암호화합니다. 이동식 저장소를 삽입할 때마다 스캔이 발생하므로, EMS에서는 인증 없이 추가된 파일을 모두 확인할 수 있습니다. 인증을 거부해도 이동식 저장소에 파일을 추가할 수 있지만 암호화된 데이터에는 액세스할 수 없습니다. 추가된 파일은 이 경우 암호화되지 않으므로 다음에 암호화된 데이터를 사용할 이동식 미디어에 인증할 때 EMS가 암호화하지 않고 추가되었을 수도 있는 모든 파일을 스캔 및 암호화합니다.
EMS Shield로 보호되지 않은 장치의 암호화된 데이터에 대한 액세스	참									참으로 설정하면 끝점 암호화 여부에 관계없이 사용자가 이동식 저장소에 있는 암호화된 데이터에 액세스할 수 있습니다.
EMS 장치 허용 목록										이 정책을 사용하면 외부 미디어 장치의 사양을 EMS 암호화에서 제외할 수 있습니다. 이 목록에 없는 외부 매체 장치는 보호됩니다. PNPDeviceID별로 최대 500자를 사용할 수 있으며, 최대 150대의 장치가 허용됩니다. 전체 최대 2048자가 허용됩니다. 이동식 저장소에 대해 PNPDeviceID를 찾기: 1 Shield로 보호된 컴퓨터에 이동식 저장 장치를 삽입합니다. 2 C:\Programdata\Dell\Dell Data Protection\Encryption\EMS에서 EMSService.log를 엽니다. 3 "PNPDeviceID="을 찾습니다. 예: 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR\DISK&VEN_SEAGATE&

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
										PROD_USB&REV_0409\2HC015KJ&0 EMS 장치 허용 목록 정책에서 다음을 지정합니다. VEN=Vendor(예: USBSTOR\DISK&VEN_SEAGATE) PROD=Product/Model Name(예: &PROD_USB). 또한 Seagate의 모든 USB 드라이브를 EMS Encryption에서 배제합니다. VEN 값(예: USBSTOR\DISK&VEN_SEAGATE)이 이 값을 앞서야만 합니다. REV=Firmware Revision(예: &REV_0409). 또한 사용되는 특정 모델을 배제합니다. VEN 및 PROD 값이 이 값을 앞서야만 합니다. 일련 번호(예: \2HC015KJ&0). 이 장치만 배제합니다. VEN, PROD 및 REV 값이 이 값을 앞서야만 합니다. 허용되는 구분 기호: 탭, 쉼표, 세미콜론, 16진수 문자 0x1E(레코드 구분 문자)
EMS 암호에 알파벳 필요	참									"참"이면 암호에 1개 이상의 글자가 필요합니다.
EMS 암호에 대/소문자 혼합 필요	참	거짓								참이면 암호에 대문자와 소문자가 최소 1개씩 필요합니다.
EMS 암호에 필요한 문자 수	8					6		8		1-40자 암호에 필요한 문자의 최소 개수입니다.
EMS 암호에 숫자 필요	참	거짓								"참"이면 암호에 1개 이상의 숫자가 필요합니다.
EMS 허용되는 암호 시도 횟수	2	3				4		3		1-10 사용자가 올바른 암호 입력을 시도할 수 있는 횟수입니다.

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
EMS 암호에 특수 문자 필요	참	거짓							참	"참"이면 암호에 1개 이상의 특수 문자가 필요합니다.
EMS 대기 시간 지연	30									0-5000초 사용자가 액세스 코드 입력 시도의 첫 번째와 두 번째 회차 사이에 기다려야 하는 시간(초)입니다.
EMS 대기 시간 증분	30	20				10	30	10		0-5000초 사용자가 각 액세스 코드 입력 시도 실패 이후에 이전 대기 시간에 추가할 증분 시간입니다.
EMS 암호화 규칙										특정 드라이브, 디렉터리 및 폴더를 암호화/암호화하지 않기 위한 암호화 규칙입니다. 총 2048자를 사용할 수 있습니다. 행 간에 라인을 추가하는 데 사용한 Space 및 Enter 문자도 사용된 문자로 계수됩니다. 2048자 제한을 초과하는 규칙은 모두 무시됩니다. Firewire, USB, eSATA 등과 같은 다중 인터페이스 연결을 통합하는 저장소 장치에서는 EMS와 암호화 규칙을 모두 사용해야 장치를 암호화할 수 있습니다. 이는 Windows 운영 체제에서 인터페이스 유형을 기준으로 한 저장 장치를 처리하는 방식에 차이가 있기 때문에 필요합니다. EMS로 iPod을 암호화하는 방법을 참조합니다.
EMS Shield로 보호되지 않은 미디어에 대한 액세스 차단	참								거짓	17MB 미만의 이동식 저장소에 대한 액세스를 차단하므로 이동식 미디어 Shield(예: 1.44MB 플로피 디스크)를 호스트할 저장소 용량이 부족합니다. 외부 미디어 암호화와 이 정책이 모두 참이면 모든 액세스가 차단됩니다. 외부 미디어 암호화가 "참"이지만 이 정책이 "거짓"이면 암호화할 수 없는 이동식 저장소에서 데이터를 읽을 수 있지만 미디어

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
										에 대한 쓰기 액세스가 차단됩니다. 외부 미디어 암호화가 "거짓"이면 이 정책은 영향을 주지 않으며 암호화할 수 없는 이동식 저장소에 대한 액세스에 영향을 주지 않습니다.
사용자 환경 제어 정책										
업데이트 시 재부팅 강제 실행	참								거짓	이 값을 참으로 설정하면 컴퓨터는 즉시 재부팅되어 암호화 프로세스 또는 SDE(시스템 데이터 암호화)와 같이 장치 기반 정책에 관련된 업데이트를 허용합니다.
개별 재부팅 연기 기간	5	10				20		15		사용자가 장치 기반 정책을 위해 재부팅 지연을 선택한 경우 지연될 기간(분)
허용되는 재부팅 연기 횟수	1					5		3		장치 기반 정책에 따라 사용자에게 재부팅 연기가 허용되는 시간.
파일 경합 알림 표시 안 함	거짓									이 정책은 응용 프로그램이 클라이언트가 처리 중인 파일에 액세스하려고 시도하는 경우 사용자에게 알림 팝업을 표시할지 여부를 제어합니다.
로컬 암호화 처리 제어 표시	거짓		참					거짓		이 값을 참으로 설정하면 사용자에게 Shield에서 현재 수행 중인 작업에 따라 암호화/암호화 해제를 일시 중지/다시 시작을 수행할 수 있는 메뉴 옵션이 시스템 트레이 아이콘으로 표시됩니다. **노트: 사용자가 암호화를 일시 중지할 수 있도록 허용하면 사용자가 Shield에서 정책별로 데이터가 완전히 암호화되거나 암호화가 해제되지 못하도록 방지할 수 있습니다.**
화면이 잠겨 있을 때만 암호화 처리 허용	거짓		사용자 선택 사항					거짓		참, 거짓, 사용자 선택 사항 "참"이면 사용자가 작업하는 동안 데이터가 암호화되거나 암호 해독되지 않습니다. 클라이언트는 화면이 잠겨 있을 때만 데이터를 처리합니다.

정책	모든 고정 드라이브 및 외부 드라이브의 적극적 보호	PCI 규제	데이터 위반 규제	HIPAA 규제	모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호	모든 고정 드라이브의 기본 보호	시스템 드라이브만 기본 보호	외부 드라이브의 기본 보호	암호화 사용 안 함	설명
										사용자 선택 사항은 시스템 트레이 아이콘에 사용자가 이 기능을 설정하거나 해제할 수 있는 옵션을 추가합니다. "거짓"이면 암호화 처리가 항상 발생합니다. 사용자가 작업하는 동안에도 마찬가지입니다. 이 옵션을 사용하면 암호화 또는 암호 해독을 완료하는 데 걸리는 시간이 대폭 늘어납니다.

템플릿 설명

모든 고정 드라이브 및 외부 드라이브의 적극적 보호

이 정책 템플릿은 기업 전체에 걸쳐 보안을 강화하고 위험을 피하는 것을 주요 목표로 삼고 있는 조직을 위해 고안되었습니다. 이는 보안이 사용성보다 더욱 중요하고 특정 사용자, 그룹 또는 장치에 대해 예외적으로 느슨한 보안 정책을 실시할 필요성이 극히 적은 경우에 효과적입니다.

이 정책 템플릿이 제공하는 기능:

- 제한성이 높은 구성을 통한 보호 강화
- 시스템 드라이브 및 모든 고정 드라이브 보호
- 이동식 저장소 장치의 모든 데이터를 암호화하고 암호화하지 않은 이동식 저장소 장치의 사용 방지
- 읽기 전용 광 드라이브 제어

PCI 규제 대상

지불카드협회 데이터보안 표준(PCI DSS)은 보안 관리, 정책, 절차, 네트워크 아키텍처, 소프트웨어 설계 및 다른 중요한 보호 조치에 대한 요구 사항을 비롯한 다면적 보안 표준입니다. 이 종합적 표준의 목적은 조직이 고객의 계정 데이터를 사전에 보호하기 위한 지침을 설정하도록 하는 데 있습니다.

이 정책 템플릿이 제공하는 기능:

- 시스템 드라이브 및 모든 고정 드라이브 보호
- 사용자에게 이동식 저장소 장치를 암호화하도록 메시지 표시
- UDF CD/DVD만 쓰기 가능 포트 제어 구성을 통해 모든 광 드라이브에 읽기 액세스 허용

데이터 위반 규제 대상

사베인-옥슬리법에 의거하여 재무 정보를 적절히 통제해야 합니다. 이 정보의 대다수가 전자 형식으로 되어 있으므로 암호화는 해당 데이터의 저장 및 전송 시 핵심 통제 요소가 됩니다. 그램-리치-블라일리(GLB)법(금융서비스현대화법) 지침에 따르면 암호화가 필수

요구 사항은 아닙니다. 그러나 연방금융기관검사위원회(FFIEC)에서는, 캘리포니아 주민의 신원 도용 방지를 위해 조직은 컴퓨터 보안 침해 발생 시 해당 내용을 모든 관련 개인에게 공지해야 한다고 제정한 캘리포니아 상원 법안 1386(캘리포니아 데이터베이스 보안 침해 고지법)에 준하여 "금융 기관은 저장된 또는 전송 중인 민감한 정보에 대한 공개 또는 변경 위험을 줄이기 위해 암호화를 반드시 도입"하도록 권장합니다. 조직이 고객에게 보안 침해 발생을 공지하지 않을 수 있는 유일한 방법은 보안 침해가 발생하기 전에 모든 개인 정보를 암호화하는 것입니다.

이 정책 템플릿이 제공하는 기능:

시스템 드라이브 및 모든 고정 드라이브 보호
사용자에게 이동식 저장소 장치를 암호화하도록 메시지 표시
UDF CD/DVD만 쓰기 가능 포트 제어 구성을 통해 모든 광 드라이브에 읽기 액세스 허용

HIPAA 규제 대상

건강보험 양도 및 책임에 관한 법안(HIPAA)은 의료 기관이 모든 개인 식별 건강 정보의 기밀성과 무결성을 보호하기 위해 다양한 기술적 보호 수단을 실행하도록 규정하고 있습니다.

이 정책 템플릿이 제공하는 기능:

시스템 드라이브 및 모든 고정 드라이브 보호
사용자에게 이동식 저장소 장치를 암호화하도록 메시지 표시
UDF CD/DVD만 쓰기 가능 포트 제어 구성을 통해 모든 광 드라이브에 읽기 액세스 허용

모든 고정 드라이브 및 외부 드라이브(기본)의 기본 보호

이 정책 템플릿은 시스템 사용성에 큰 영향을 주지 않고도 높은 수준으로 보호해 주는 권장 구성을 제공합니다.

이 정책 템플릿이 제공하는 기능:

시스템 드라이브 및 모든 고정 드라이브 보호
사용자에게 이동식 저장소 장치를 암호화하도록 메시지 표시
UDF CD/DVD만 쓰기 가능 포트 제어 구성을 통해 모든 광 드라이브에 읽기 액세스 허용

모든 고정 드라이브의 기본 보호

이 정책 템플릿이 제공하는 기능:

시스템 드라이브 및 모든 고정 드라이브 보호
모든 지원 형식으로 CD/DVD 쓰기 가능. 포트 제어 구성을 통해 모든 광 드라이브에 읽기 액세스 허용

이 정책 템플릿이 제공하지 않는 기능:
이동식 저장소 장치 암호화

시스템 드라이브만 기본 보호

이 정책 템플릿이 제공하는 기능:

시스템 드라이브(일반적으로 운영 체제가 로드되는 C: 드라이브) 보호
모든 지원 형식으로 CD/DVD 쓰기 가능. 포트 제어 구성을 통해 모든 광 드라이브에 읽기 액세스 허용

이 정책 템플릿이 제공하지 않는 기능:

외부 드라이브의 기본 보호

이 정책 템플릿이 제공하는 기능:

이동식 저장소 장치 보호

UDF CD/DVD만 쓰기 가능 포트 제어 구성을 통해 모든 광 드라이브에 읽기 액세스 허용

이 정책 템플릿이 제공하지 않는 기능:

시스템 드라이브(일반적으로 운영 체제가 로드되는 C: 드라이브) 또는 다른 고정 드라이브 보호

암호화 사용 안 함

이 정책 템플릿은 암호화 보호를 제공하지 않습니다. 이 템플릿 사용 시 장치 손실 및 도난을 방지하려면 추가 조치를 취하십시오.

이 템플릿은 활성 암호화 없이 보안 변경을 시작하려는 조직에 유용합니다. 조직의 배포가 편리해짐에 따라, 개별 정책을 조정하거나 조직의 일부 또는 전체의 템플릿을 더욱 강력하게 적용하여 암호화를 천천히 사용할 수 있습니다.

일회용 암호의 설치 전 구성으로 진행합니다.

10

일회용 암호의 설치 전 구성

설치를 시작하기 **전에** 다음과 같은 Personal Edition 기능을 구성해야 합니다.

TPM 초기화

- 로컬 관리자 그룹(또는 이와 동등)의 구성원이어야 합니다.
- 컴퓨터에 호환되는 BIOS 및 TPM이 장착되어 있어야 합니다.

이 작업은 OTP(일회용 암호)를 사용하는 경우에 필요합니다.

- http://technet.microsoft.com/en-us/library/cc753140.aspx의 지침을 따릅니다.

마스터 설치 프로그램에서 하위 설치 프로그램 추출

- 각 클라이언트를 개별적으로 설치하려면 설치 프로그램에서 하위 실행 파일을 추출합니다.
- 마스터 설치 프로그램을 사용하여 설치한 경우에는 클라이언트를 개별적으로 설치 제거해야 합니다. 클라이언트를 설치 제거할 수 있도록 이 프로세스에 따라 마스터 설치 프로그램에서 클라이언트를 추출하십시오.

1 Dell 설치 미디어에서 `DDPSetup.exe` 파일을 로컬 컴퓨터로 복사합니다.

2 `DDPSetup.exe` 파일과 동일한 위치에서 명령 프롬프트를 열고 다음을 입력합니다.

```
DDPSetup.exe /z"\"EXTRACT_INSTALLERS=C:\extracted\""
```

추출 경로는 63자를 초과할 수 없습니다.

설치를 시작하기 전에 설치하고자 하는 각 하위 설치 프로그램에 필요한 모든 필수 조건이 충족되었고 필요한 모든 소프트웨어가 설치되었는지 확인하십시오. 자세한 내용은 요구 사항을 참조하십시오.

추출된 하위 설치 프로그램은 C:\extracted\.에 있습니다.

문제 해결로 진행합니다.

문제 해결

Windows 10 Anniversary Update로 업그레이드

Encryption이 설치된 컴퓨터는 특별 구성된 Windows 10 Upgrade 패키지를 사용해 Windows 10 Anniversary Update로 업그레이드해야 합니다. 구성된 버전의 업그레이드 패키지는 Dell Data Protection이 암호화 파일에 대한 액세스를 관리하여, 업그레이드 프로세스 동안 파일이 손상되지 않도록 해줍니다.

Windows 10 Anniversary 버전으로 업그레이드하려면 다음 문서의 지침을 따르십시오.

http://www.dell.com/support/article/us/en/19/SLN298382

Encryption 클라이언트 문제 해결

Windows 10 Anniversary Update로 업그레이드

Windows 10 Anniversary Update 버전으로 업그레이드하려면 다음 문서의 지침을 따르십시오. http://www.dell.com/support/article/us/en/19/SLN298382.

(선택 사항) Encryption Removal Agent 로그 파일 생성

- 설치 제거 프로세스를 시작하기 전에 선택적으로 Encryption Removal Agent 로그 파일을 생성할 수 있습니다. 이 로그 파일은 설치 제거/암호 해독 작업의 문제를 해결하는 데 유용합니다. 설치 제거 프로세스 중 파일을 암호 해독하지 않으려면 이 로그 파일을 만들지 않아도 됩니다.
- Encryption Removal Agent 로그 파일은 Encryption Removal Agent 서비스가 실행될 때까지 생성되지 않으며, 이 서비스는 컴퓨터를 다시 시작해야 실행됩니다. 클라이언트가 성공적으로 설치 제거되고 컴퓨터가 완전히 암호 해독되면 로그 파일이 영구적으로 삭제됩니다.
- 로그 파일 경로는 **C:\ProgramData\Dell\Dell Data Protection\Encryption.**입니다.
- 암호 해독 대상 컴퓨터에 다음과 같은 레지스트리 항목을 만듭니다.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=dword:2

  0: 로깅하지 않음

  1: 서비스가 실행되지 않는 오류 로깅

  2: 전체 데이터 암호 해독이 안 되는 오류 로깅(권장 수준)

  3: 모든 암호 해독 볼륨 및 파일에 대한 정보 로깅

  5: 디버깅 정보 로깅

TSS 버전 찾기

- TSS는 TPM과 상호 작용하는 요소입니다. TSS 버전을 찾으려면 C:\Program Files\Dell\Dell Data Protection\Drivers\TSS\bin > tcsd_win32.exe(기본 위치)로 이동합니다. 파일을 마우스 오른쪽 단추로 클릭하고 **속성**을 선택합니다. **세부 정보** 탭에서 파일 버전을 확인합니다.

EMS와 PCS 상호 작용

미디어가 읽기 전용이 아니고 포트가 차단되지 않았는지 확인하려면

포트 제어 시스템과 상호 작용하는 EMS Shield로 보호되지 않은 미디어에 대한 액세스 정책- 저장소 클래스: 외부 드라이브 제어 정책. 보호되지 않는 미디어 정책에 EMS 액세스를 *전체 액세스로* 설정하려는 경우, 저장소 클래스: 외부 드라이브 제어 정책 또한 *전체 액세스*로 설정되어 미디어가 읽기 전용으로 설정되지 않고 포트가 차단되지 않았는지 확인합니다.

CD/DVD에 쓴 데이터를 암호화하려면

- EMS 외부 미디어 암호화 = 참을 설정합니다.
- EMS CD/DVD 암호화 제외 = 거짓을 설정합니다.
- 하위 클래스 저장소: 광학 드라이브 제어 = UDF 전용으로 설정합니다.

WSScan 사용

- WSScan을 사용하면 Encryption 클라이언트를 설치 제거할 때 모든 데이터가 해독되는지 확인할 수 있을 뿐 아니라 암호화 상태를 보고 암호화해야 하는 암호화되지 않은 파일을 식별할 수 있습니다.
- 이 유틸리티를 실행하려면 관리자 권한이 필요합니다.

WSScan

1 Dell 설치 미디어에서 스캔할 Windows 컴퓨터로 WSScan.exe를 복사합니다.
2 해당 위치에서 명령줄을 실행하고 프롬프트가 표시되면 **wsscan.exe**를 입력합니다. WSScan이 실행됩니다.
3 **고급**을 클릭합니다.
4 드롭다운 메뉴에서 스캔할 드라이브의 유형을 선택합니다(*모든 드라이브*, *고정 드라이브*, *이동식 드라이브* 또는 *CDROM/DVDROM*).
5 드롭다운 메뉴에서 원하는 암호화 보고서 유형을 선택합니다(*암호화된 파일*, *암호화되지 않은 파일*, *모든 파일* 또는 *위반되는 암호화되지 않은 파일*).
   - *암호화된 파일* - Encryption 클라이언트를 설치 제거할 때 모든 데이터가 해독되는지 확인합니다. 암호 해독 정책 업데이트 실행 등의 기존 데이터 암호 해독 프로세스를 따릅니다. 데이터를 암호 해독한 후에는 설치 제거를 준비하는 단계에서 재시작을 수행하기 전에 WSScan를 실행하여 모든 데이터가 암호 해독되었는지 확인합니다.
   - *암호화되지 않은 파일* - 암호화되지 않은 파일을 식별합니다. 파일을 암호화해야 하는지 여부(Y/N)가 함께 표시됩니다.
   - *모든 파일* - 암호화된 파일과 그렇지 않은 모든 파일을 나열합니다. 파일을 암호화해야 하는지 여부(Y/N)가 함께 표시됩니다.
   - *위반되는 암호화되지 않은 파일* - 암호화해야 하지만 암호화되지 않은 파일을 식별합니다.
6 **검색**을 클릭합니다.

또는

1 **고급**을 클릭하여 보기 모드를 **간단히**로 전환하여 특정 폴더를 스캔합니다.
2 검색 설정으로 이동하고 **경로 검색** 필드에 폴더 경로를 입력합니다. 이 필드를 사용할 경우 드롭다운 상자에 선택한 사항이 무시됩니다.
3 WSScan 출력을 파일에 쓰지 않으려는 경우 **파일로 출력** 확인란의 선택을 취소합니다.
4 필요할 경우 *경로*에서 기본 경로와 파일 이름을 변경합니다.
5 기존 WSScan 출력 파일을 덮어쓰지 않으려는 경우 **기존 파일에 추가**을 선택합니다.

6 다음과 같이 출력 형식을 선택합니다.

- 스캔된 출력을 보고서 형식의 목록으로 표시하려면 "보고서 형식"을 선택합니다. 이 모드가 기본 형식입니다.
- 스프레드시트 응용 프로그램으로 가져올 수 있는 출력을 사용하려면 "값 구분 파일"을 선택합니다. 기본 구분 기호는 "|"이며, 최대 9자의 영숫자, 공백 또는 키보드 문장 부호 문자로 변경할 수 있습니다.
- 각 값을 큰따옴표 표시 안에 포함하려면 "따옴표 붙은 값"을 선택합니다.
- 암호화된 각 파일에 대해 고정 길이의 정보 행이 연속적으로 포함되어 있고 구분 기호로 구분되지 않은 출력을 사용하려면 "고정 너비 파일"을 선택합니다.

7 **검색**을 클릭합니다.

검색을 중지하려면 **검색 중지**를 클릭합니다. 표시된 메시지를 지우려면 **지우기**를 클릭합니다.

WSScan 출력

암호화된 파일에 대한 WSScan 정보에는 다음 정보가 포함되어 있습니다.

출력 예제:

[2015-07-28 07:52:33] SysData.7vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" is still AES256 encrypted

출력	의미
날짜/시간 스탬프	파일을 스캔한 날짜와 시간입니다.
암호화 유형	파일 암호화에 사용한 암호화 유형입니다. **SysData:** SDE 암호화 키입니다. **User:** 사용자 암호화 키입니다. **Common:** 일반적인 암호화 키입니다. WSScan은 공유를 위한 암호화를 사용하여 암호화된 파일을 보고하지 않습니다.
KCID	키 컴퓨터 ID입니다. 위의 예에서와 같이, **"7vdlxrsb"**입니다. 매핑된 네트워크 드라이브를 스캔하는 경우 스캔 보고서가 KCID를 반환하지 않습니다.
UCID	사용자 ID입니다. 위의 예에서와 같이, **"_SDENCR_"**입니다. UCID는 해당 컴퓨터의 모든 사용자가 공유합니다.
파일	암호화된 파일의 경로입니다. 위의 예에서와 같이, **"c:\temp\Dell - test.log"**입니다.
알고리즘	파일을 암호화하는 데 사용하는 암호화 알고리즘입니다. 위의 예에서와 같이, **"is still AES256 encrypted"**입니다. Rijndael 128 Rijndael 256 AES 128 AES 256

출력	의미
	3DES

Encryption Removal Agent 상태 확인

Encryption Removal Agent에서 다음과 같이 해당 상태가 서비스 패널(시작 > 실행... > services.msc > 확인)의 설명 영역에 표시됩니다. 서비스를 정기적으로 새로 고쳐(서비스 강조 표시 > 마우스 오른쪽 단추 클릭 > 새로 고침) 상태를 업데이트합니다.

- **SDE 비활성화 대기 중** – Encryption 클라이언트가 설치 또는 구성되어 있거나, 둘 다에 해당합니다. Encryption 클라이언트가 제거될 때까지 암호 해독이 시작되지 않습니다.
- **초기 스윕** – 서비스가 초기 스윕을 실행하면서 암호화된 파일과 바이트 수를 계산합니다. 초기 스윕은 한 번만 실행됩니다.
- **암호 해독 스윕** – 서비스가 파일을 암호 해독하고 있으며 잠겨 있는 파일의 암호 해독을 요청할 수도 있습니다.
- **재부팅 시 암호 해독(부분적)** – 암호 해독 스윕이 완료되었으며 다음에 다시 시작하면 잠겨 있는 파일이 일부만 암호 해독됩니다.
- **재부팅 시 암호 해독** – 암호 해독 스윕이 완료되었으며 다음에 다시 시작하면 잠긴 파일이 모두 암호 해독됩니다.
- **모든 파일을 암호 해독할 수 없음** – 암호 해독 스윕이 완료되었지만 모든 파일을 암호 해독할 수 없습니다. 이 상태는 다음 중 하나가 발생했음을 의미합니다.
  - 잠긴 파일이 너무 크거나 잠금 해제를 요청하는 중 오류가 발생하여 잠긴 파일의 암호 해독을 예약할 수 없습니다.
  - 파일을 암호 해독하는 중 입력/출력 오류가 발생했습니다.
  - 정책으로 파일을 암호 해독할 수 없습니다.
  - 파일을 암호화해야 한다는 내용이 표시되었습니다.
  - 암호 해독 스윕 중 오류가 발생했습니다.
  - LogVerbosity=2(또는 이상)가 설정되어 있으면 항상 로그 파일이 생성됩니다(로깅이 구성된 경우). 문제를 해결하려면 로그의 자세한 정도를 2로 설정하고 Encryption Removal Agent 서비스를 다시 시작해서 암호 해독 스윕을 한 번 더 강제 실행합니다.
- **완료** – 암호 해독 스윕이 완료되었습니다. 다음에 다시 시작할 때 서비스, 실행 파일, 드라이버 및 드라이버 실행 파일이 모두 삭제되도록 예약됩니다.

EMS로 iPod을 암호화하는 방법

이러한 규칙은 iPod뿐 아니라 모든 이동식 장치에서 이러한 폴더와 파일 형식을 대상으로 암호화를 사용하거나 사용하지 않도록 설정합니다. 규칙을 정의할 때는 주의하십시오.

- iPod Shuffle의 경우 예기치 않은 결과가 발생할 수 있어 권장하지 않습니다.
- iPod이 변경되면 이 정보도 변경될 수 있으므로 EMS를 사용하는 컴퓨터에서 iPod 사용을 허용할 때 주의해야 합니다.
- iPod의 폴더 이름은 iPod 모델에 따라 다르므로 모든 iPod 모델에서 모든 폴더 이름을 포함하는 제외 정책을 만드는 것이 좋습니다.
- EMS를 통해 iPod을 암호화하면 iPod을 사용할 수 없게 되는지 확인하려면 EMS 암호화 규칙 정책에 다음 규칙을 입력하십시오.

  -R#:\Calendars

  -R#:\Contacts

  -R#:\iPod_Control

  -R#:\Notes

  -R#:\Photos
- 위의 디렉터리에 특정 파일 형식에 대한 암호화를 강제로 적용할 수도 있습니다. 다음 규칙을 추가하면 ppt, pptx, doc, docx, xls 및 xlsx 파일이 이전 규칙을 통해 암호화에서 *제외된* 디렉터리에 암호화됩니다.

  ^R#:\Calendars;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Contacts;ppt.doc.xls.pptx.docx.xlsx

^R#:\iPod_Control;ppt.doc.xls.pptx.docx.xlsx

^R#:\Notes;ppt.doc.xls.pptx.docx.xlsx

^R#:\Photos;ppt.doc.xls.pptx.docx.xlsx

- 이러한 5개 규칙을 다음 규칙으로 바꾸면 캘린더, 연락처, iPod_Control, 메모 및 사진을 포함하여 iPod 디렉터리에 있는 ppt, pptx, doc, docx, xls 및 xlsx 파일에 암호화가 적용됩니다.

^R#:\;ppt.doc.xls.pptx.docx.xlsx

- 규칙은 다음 iPod에 대해 테스트되었습니다.

iPod Video 30gb 5세대

iPod Nano 2gb 2세대

iPod Mini 4gb 2세대

Dell ControlVault 드라이버

Dell ControlVault 드라이버 및 펌웨어 업데이트

출하 시 Dell 컴퓨터에 설치된 Dell ControlVault 드라이버 및 펌웨어는 오래되었으며 다음 절차에 따라 다음 순서대로 업데이트해야 합니다.

클라이언트를 설치하는 동안 Dell ControlVault 드라이버를 업데이트하기 위해 설치 프로그램을 종료하라는 오류 메시지가 표시되면, 이 메시지를 안전하게 해제하여 클라이언트 설치를 계속할 수 있습니다. Dell ControlVault 드라이버 (및 펌웨어)는 클라이언트 설치를 완료한 후에 업데이트할 수 있습니다.

최신 드라이버 다운로드

1 support.dell.com으로 이동합니다.
2 컴퓨터 모델을 선택합니다.
3 **드라이버 및 다운로드**를 선택합니다.
4 대상 컴퓨터의 **운영 체제**를 선택합니다.
5 **보안** 범주를 확장합니다.
6 Dell ControlVault 드라이버를 다운로드하고 저장합니다.
7 Dell ControlVault 펌웨어를 다운로드하고 저장합니다.
8 필요한 경우, 드라이버와 펌웨어를 대상 컴퓨터에 복사합니다.

Dell ControlVault 드라이버 설치

드라이버 설치 파일을 다운로드한 폴더로 이동합니다.

Dell ControlVault 드라이버를 더블 클릭하여 자동 압축 해제 실행 파일을 시작합니다.

:

반드시 드라이버부터 설치하십시오. *이 문서 생성 시* 드라이버의 파일 이름은 ControlVault_Setup_2MYJC_A37_ZPE.exe입니다.

계속을 클릭하여 시작합니다.

확인을 클릭하여 기본 위치인 C:\Dell\Drivers\<New Folder>에 드라이버 파일들을 압축 해제합니다.

예를 클릭하여 새 폴더 생성을 허용합니다.

성공적으로 압축 해제했다는 메시지가 표시되면 **확인**을 클릭합니다.

압축 해제가 끝나면 파일들이 들어 있는 폴더가 표시될 것입니다. 그렇지 않다면, 파일들을 추출한 폴더로 이동하십시오. 이 경우, 폴더는 **JW22F**입니다.

CVHCI64.MSI를 더블 클릭하여 드라이버 설치 프로그램을 시작합니다. [이 예에서는 **CVHCI64.MSI**가 보기로 나옵니다.(32비트 컴퓨터에서는 CVHCI)]

시작 화면에서 **다음**을 클릭합니다.

다음을 클릭하여 기본 위치인 C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.에 드라이버를 설치합니다.

완료 옵션을 선택하고 **다음**을 클릭합니다.

설치을 클릭하여 드라이버 설치를 시작합니다.

필요에 따라, 설치 프로그램 로그 파일을 표시하기 위해 확인란을 선택합니다. **마침**을 클릭하여 마법사를 종료합니다.

드라이버 설치 확인

운영 체제 및 하드웨어 구성에 따라 장치 관리자에 Dell ControlVault 장치 (및 기타 장치)가 있을 것입니다.

Dell ControlVault 펌웨어 설치

1 펌웨어 설치 파일을 다운로드한 폴더로 이동합니다.
2 Dell ControlVault 펌웨어를 더블 클릭하여 자동 압축 해제 실행 파일을 시작합니다.
3 **계속**을 클릭하여 시작합니다.
4 **확인**을 클릭하여 기본 위치인 C:\Dell\Drivers\<New Folder>에 드라이버 파일들을 압축 해제합니다.
5 **예**를 클릭하여 새 폴더 생성을 허용합니다.
6 성공적으로 압축 해제했다는 메시지가 표시되면 **확인**을 클릭합니다.
7 압축 해제가 끝나면 파일들이 들어 있는 폴더가 표시될 것입니다. 그렇지 않다면, 파일들을 추출한 폴더로 이동하십시오. **펌웨어** 폴더를 선택합니다.
8 **ushupgrade.exe**를 더블 클릭하여 펌웨어 설치 프로그램을 시작합니다.
9 **시작**을 클릭하여 펌웨어 업그레이드를 시작합니다.

:

이전 버전 펌웨어를 업그레이드하는 경우, 관리자 암호를 입력하라는 요청을 받을 수 있습니다. 이 대화 상자가 표시되면 암호로 `Broadcom`을 입력하고 **Enter**를 클릭합니다.

몇 가지 상태 메시지가 표시됩니다.

10 **재시작**을 클릭하여 펌웨어 업그레이드를 완료합니다.

Dell ControlVault 드라이버 및 펌웨어 업데이트가 완료됩니다.

레지스트리 설정

이 섹션에서는 로컬 클라이언트 컴퓨터에 대해 Dell ProSupport에서 승인한 모든 레지스트리 설정에 대해 자세히 설명합니다.

Encryption 클라이언트

(선택 사항) Encryption Removal Agent 로그 파일 생성

설치 제거 프로세스를 시작하기 전에 선택적으로 Encryption Removal Agent 로그 파일을 생성할 수 있습니다. 이 로그 파일은 설치 제거/암호 해독 작업의 문제를 해결하는 데 유용합니다. 설치 제거 프로세스 중 파일을 암호 해독하지 않으려면 이 로그 파일을 만들지 않아도 됩니다.

Encryption Removal Agent 로그 파일은 Encryption Removal Agent 서비스가 실행될 때까지 생성되지 않으며, 이 서비스는 컴퓨터를 다시 시작해야 실행됩니다. 클라이언트가 성공적으로 설치 제거되고 컴퓨터가 완전히 암호 해독되면 로그 파일이 영구적으로 삭제됩니다.

로그 파일 경로는 C:\ProgramData\Dell\Dell Data Protection\Encryption.입니다.

암호 해독 대상 컴퓨터에 다음과 같은 레지스트리 항목을 만듭니다.

[HKLM\Software\Credant\DecryptionAgent]

"LogVerbosity"=dword:2

0: 로깅하지 않음

1: 서비스가 실행되지 않는 오류 로깅

2: 전체 데이터 암호 해독이 안 되는 오류 로깅(권장 수준)

3: 모든 암호 해독 볼륨 및 파일에 대한 정보 로깅

5: 디버깅 정보 로깅

Windows 로그온과 함께 스마트 카드 사용

Windows 인증과 함께 스마트 카드를 사용하려면 클라이언트 컴퓨터에서 다음 레지스트리 값을 설정해야 합니다.

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=dword:1

설치 중에 임시 파일 유지

기본적으로, 설치 중에 c:\windows\temp 디렉터리의 모든 임시 파일이 자동으로 삭제됩니다. 임시 파일이 삭제되면 초기 암호화가 신속하게 진행되며 삭제 작업은 초기 암호화 스윕이 수행되기 전에 발생합니다.

하지만 조직에서 \temp 디렉터리 내에 파일 구조를 유지해야 하는 타사 응용 프로그램을 사용하는 경우에는 이러한 삭제를 방지해야 합니다.

임시 파일 삭제를 사용하지 않으려면 다음과 같이 레지스트리 설정을 만들거나 수정하십시오.

[HKLM\SOFTWARE\CREDANT\CMGShield]

"DeleteTempFiles"=REG_DWORD:0

임시 파일을 삭제하지 않으면 초기 암호화에 시간이 더 걸립니다.

암호화를 시작하거나 연기하도록 사용자 메시지에 대한 기본 동작 변경

Encryption 클라이언트는 업데이트가 수행될 때마다 *length of each policy update delay(각 정책 업데이트 연기 시간)* 메시지를 5분 동안 표시합니다. 사용자가 메시지에 응답하지 않으면 다음 지연이 시작됩니다. 최종 연기 메시지에 카운트다운 및 진행률 표시줄이 포함되고, 사용자가 응답하거나 최종 연기가 만료되고 필요한 로그오프/재부팅이 수행될 때까지 해당 메시지가 표시됩니다.

사용자가 메시지에 응답하지 않으면 암호화가 처리되지 않도록 방지하기 위해 암호화를 시작하거나 지연하도록 사용자 메시지의 동작을 변경할 수 있습니다. 이렇게 하려면 레지스트리를 다음 값으로 설정하십시오.

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"SnoozeBeforeSweep"=DWORD:1

0이 아닌 값을 사용하면 기본 동작이 다시 알림으로 변경됩니다. 사용자가 상호 작용하지 않으면 구성 가능한 허용 연기 횟수까지 암호화 처리가 연기됩니다 마지막 연기 시간이 끝나면 암호화 처리가 시작됩니다.

다음과 같이 최대 연기 시간을 계산합니다(사용자가 5분 동안 표시되는 각 지연 메시지에 응답하지 않을 경우 최대 시간 동안 지연됨).

(허용되는 정책 업데이트 연기 횟수 × 각 정책 업데이트 연기 시간) + (5분 × [허용되는 정책 업데이트 연기 횟수 - 1])

SDUser 키의 기본 사용 변경

SDE(System Data Encryption)는 SDE 암호화 규칙에 대한 정책 값에 따라 적용됩니다. 추가 디렉터리는 SDE 암호 기능 활성화 정책이 선택되어 있는 경우 기본적으로 보호됩니다. 자세한 내용은 AdminHelp에서 "SDE 암호화 규칙"을 검색하십시오. Encryption 클라이언트가 활성 SDE 정책이 포함된 정책 업데이트를 처리하면, SDE 키(장치 키)가 아닌 SDUser 키(사용자 키)로 현재 사용자 프로필 디렉터리가 기본적으로 암호화됩니다. SDE로 암호화되지 않은 사용자 디렉터리로 복사되는(이동 아님) 파일 또는 폴더를 암호화하는 데에도 이 SDUser 키가 사용됩니다.

SDUser 키를 비활성화하여 SDE 키를 사용해 이러한 사용자 디렉터리를 암호화하려면, 컴퓨터에서 다음 레지스트리 항목을 생성하십시오.

[HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

"EnableSDUserKeyUsage"=dword:00000000

이 레지스트리 키가 없거나 0 이외의 다른 값으로 설정되어 있으면, SDUser 키가 이러한 사용자 디렉터리를 암호화하는 데 사용됩니다.

Advanced Authentication 클라이언트

스마트 카드 및 생체 인식 서비스 사용 안 함(선택 사항)

Security Tools가 스마트 카드 및 생체 인식 장치와 관련된 서비스의 시작 유형을 "자동"으로 변경하지 않도록 서비스 시작 기능을 사용하지 않을 수 있습니다.

이 기능을 비활성화하면 Security Tools가 다음 세 가지 서비스를 시작하지 않습니다.

SCardSvr - 컴퓨터가 판독하는 스마트 카드에 대한 액세스를 관리합니다. 이 서비스가 중지되면 컴퓨터에서 스마트 카드를 판독할 수 없습니다. 이 서비스가 비활성화되면 서비스에 명시적으로 의존된 모든 서비스가 시작되지 않습니다.

SCPolicySvc - 스마트 카드가 제거되면 사용자의 데스크톱이 잠기도록 시스템을 구성할 수 있습니다.

WbioSrvc - Windows 생체 인식 서비스를 통해 클라이언트 응용 프로그램은 생체 인식 하드웨어 또는 샘플에 직접 액세스하지 않고도 생체 인식 데이터를 캡처, 비교, 조종, 저장할 수 있습니다. 이 서비스는 권한이 부여된 SVCHOST 프로세스에서 호스팅됩니다.

이 기능을 비활성화하면 실행해야 하는 필요한 서비스와 관련된 경고도 표시되지 않습니다.

기본적으로 레지스트리 키가 없거나 값이 0으로 설정되어 있는 경우 이 기능이 사용됩니다.

[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

사용하려면 0으로 설정합니다.

사용하지 않으려면 1로 설정합니다.

Windows 로그온과 함께 스마트 카드 사용

Windows 인증과 함께 스마트 카드를 사용하려면 클라이언트 컴퓨터에서 다음 레지스트리 값을 설정해야 합니다.

[HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

"MSSmartcardSupport"=dword:1

용어집으로 진행합니다.

13

용어집

Advanced Authentication – Advanced Authentication 제품은 완벽하게 통합된 지문, 스마트 카드, 비접촉식 스마트 카드 판독기 옵션을 제공합니다. Advanced Authentication은 여러 가지 하드웨어 인증 방법을 관리하는 데 도움이 되며, 자체 암호화 드라이브 및 SSO를 통한 로그인을 지원하며, 사용자 자격 증명 및 암호를 관리합니다. 또한 Advanced Authentication을 사용하여 PC뿐만 아니라 모든 웹 사이트, SaaS 또는 응용 프로그램에 액세스할 수 있습니다. 사용자가 자격 증명을 등록하면 Advanced Authentication은 해당 자격 증명을 사용하여 장치에 로그온하고 암호를 변경할 수 있도록 합니다.

EAP(암호화 관리자 암호) - EAP는 각 컴퓨터에 고유한 관리자 암호입니다. 로컬 관리 콘솔에서 구성을 변경할 경우 대부분 이 암호를 입력해야 합니다. 이 암호는 데이터 복구를 위해 LSARecovery_[hostname].exe 파일을 사용할 경우 요구되는 암호와도 동일합니다. 이 암호를 기록해서 안전한 장소에 보관하십시오.

Encryption 클라이언트 – Encryption 클라이언트는 끝점이 네트워크에 연결, 네트워크에서 분리, 분실 또는 도난 여부에 따라 보안 정책을 시행하는 장치 구성 요소입니다. 끝점에 신뢰할 수 있는 컴퓨팅 환경을 생성하는 Encryption 클라이언트는 장치 운영 체제에 추가적인 보안 계층을 형성하며 인증, 암호화, 권한 부여를 일관적으로 적용함으로써 중요한 정보를 최대한 보호할 수 있습니다.

암호화 키 - 대부분의 경우 Encryption 클라이언트는 사용자 키와 추가적인 2개의 암호화 키를 사용합니다. 예외: 모든 SDE 정책 및 보안 Windows 자격 증명 정책에서는 SDE 키를 사용합니다. Encrypt Windows 페이징 파일 암호화 정책 및 보안 Windows 최대 절전 모드 파일 정책은 자체 키인 GPK(General Purpose Key)를 사용합니다. 일반 키를 사용하면 파일이 생성된 장치에서 관리되는 모든 사용자가 파일에 액세스할 수 있습니다. 사용자 키를 사용하면 파일이 생성된 장치에서만 파일을 만든 사용자만 파일에 액세스할 수 있습니다. 사용자 로밍 키를 사용하면 Shield로 보호된 Windows(또는 Mac) 장치에서 파일을 만든 사용자만 파일에 액세스할 수 있습니다.

암호화 스윕 - 암호화 스윕은 포함된 파일의 암호화 상태를 올바르게 유지하기 위해 Shield로 보호된 끝점에서 암호화될 폴더를 스캔하는 프로세스입니다. 일반 파일 생성 및 이름 변경 작업으로는 암호화 스윕이 트리거되지 않습니다. 다음과 같이 암호화 스윕이 발생할 수 있는 시기와 그에 따른 스윕 횟수에 영향을 주는 요소를 파악하는 것이 중요합니다. - 암호화 스윕은 암호화를 활성화한 정책을 처음 수신할 때 발생합니다. 이것은 정책이 암호화를 사용하는 경우 활성화 직후 발생할 수 있습니다. - 로그온 시 워크스테이션 스캔 정책이 활성화되어 있으면 암호화가 지정된 폴더는 사용자가 로그온할 때마다 스윕됩니다. - 이후의 특정 정책 변경에 따라 스윕이 다시 발생할 수 있습니다. 암호화 폴더, 암호화 알고리즘, 암호화 키 용도(일반 및 사용자)의 정의에 관한 정책을 변경하는 경우 스윕이 트리거됩니다. 또한 암호화 사용 및 해제 전환 시 암호화 스윕이 트리거됩니다.

일회용 암호(OTP) – OTP는 단 한 번만 사용할 수 있는 암호로, 제한된 기간 동안에만 유효합니다. OTP를 사용하려면 TPM을 설치하고, 활성화해야 하며, 소유권을 가지고 있어야 합니다. OTP를 이용하려면 Security Console 및 Security Tools Mobile 앱을 사용하여 모바일 장치와 컴퓨터를 페어링해야 합니다. Security Tools Mobile 앱에서 생성된 모바일 장치의 암호는 Windows 로그온 화면에서 컴퓨터에 로그온하는 데 사용됩니다. 정책에 따라, 컴퓨터에 로그온할 때 OTP를 사용한 적이 없으면 암호가 만료되거나 분실한 경우 OTP 기능을 사용하여 컴퓨터에 대한 액세스 권한을 복구할 수 있습니다. OTP 기능은 그 밖에 인증이나 복구 목적으로 사용할 수도 있지만, 이 두 가지를 동시에 지원하지는 못합니다. OTP 보안은 생성된 암호가 1회용이며 유효 기간이 짧다는 점에서 다른 인증 방식의 보안보다 강력하다고 할 수 있습니다.

PBA(부팅 전 인증) – PBA(부팅 전 인증)는 BIOS 또는 부팅 펌웨어를 확장하는 기능을 하며 운영 체제 외부에서 신뢰할 수 있는 인증 계층으로 안전한 변조 방지 환경을 보장합니다. PBA는 사용자에게 올바른 자격 증명이 있는지 확인할 때까지 하드 디스크에서 운영 체제 등의 데이터를 읽을 수 없도록 합니다.

SSO(Single Sign On) - SSO는 부팅 전 및 Windows 로그온에서 다단계 인증을 사용할 경우 로그온 프로세스를 간소화합니다. 이 기능을 사용할 경우 부팅 전에만 인증이 필요하며 사용자는 Windows에 자동으로 로그온됩니다. 사용하지 않을 경우에는 여러 번 인증이 필요할 수 있습니다.

SDE(System Data Encryption) – SDE는 운영 체제와 프로그램 파일을 암호화하도록 설계되었습니다. 이러한 목적을 달성하기 위해 운영 체제가 부팅되는 동안 SDE가 해당 키를 열 수 있어야 합니다. 목적은 운영 체제에 대한 공격자의 오프라인 공격이나 변조를 방지하는 것입니다. SDE는 사용자 데이터에 사용하기 위한 용도가 아니며, 일반 및 사용자 키 암호화는 중요한 사용자 데이터에 사용하기 위한 용도입니다. 암호화 키 잠금을 해제하려면 사용자 암호가 필요하기 때문입니다. SDE 정책은 운영 체제가 부팅 프로세스를 시작하

는 데 필요한 파일을 암호화하지 않습니다. SDE 정책은 부팅 전 인증을 요구하지 않으며 마스터 부트 레코드의 동작을 방해하지도 않습니다. 컴퓨터가 시작되면 사용자가 로그인하기 전에 암호화된 파일이 가용 상태가 되어 패치 관리, SMS, 백업 및 복구 도구를 사용할 수 있습니다. SDE 암호화를 비활성화하면 SDE 암호화 규칙 등과 같은 기타 SDE 정책과 관계 없이 관련 사용자에 대해 SDE로 암호화된 모든 파일 및 디렉터리의 자동 암호 해독이 트리거됩니다.

TPM(Trusted Platform Module) – TPM은 안전한 저장, 측정, 증명의 세 가지 주요 기능을 제공하는 보안 칩입니다. Encryption 클라이언트는 안전한 저장 기능 때문에 TPM을 사용합니다. TPM도 소프트웨어 자격 증명 모음에 대해 암호화된 컨테이너를 제공할 수 있습니다. TPM은 OTP(일회용 암호) 기능을 사용하려는 경우에도 필요합니다.